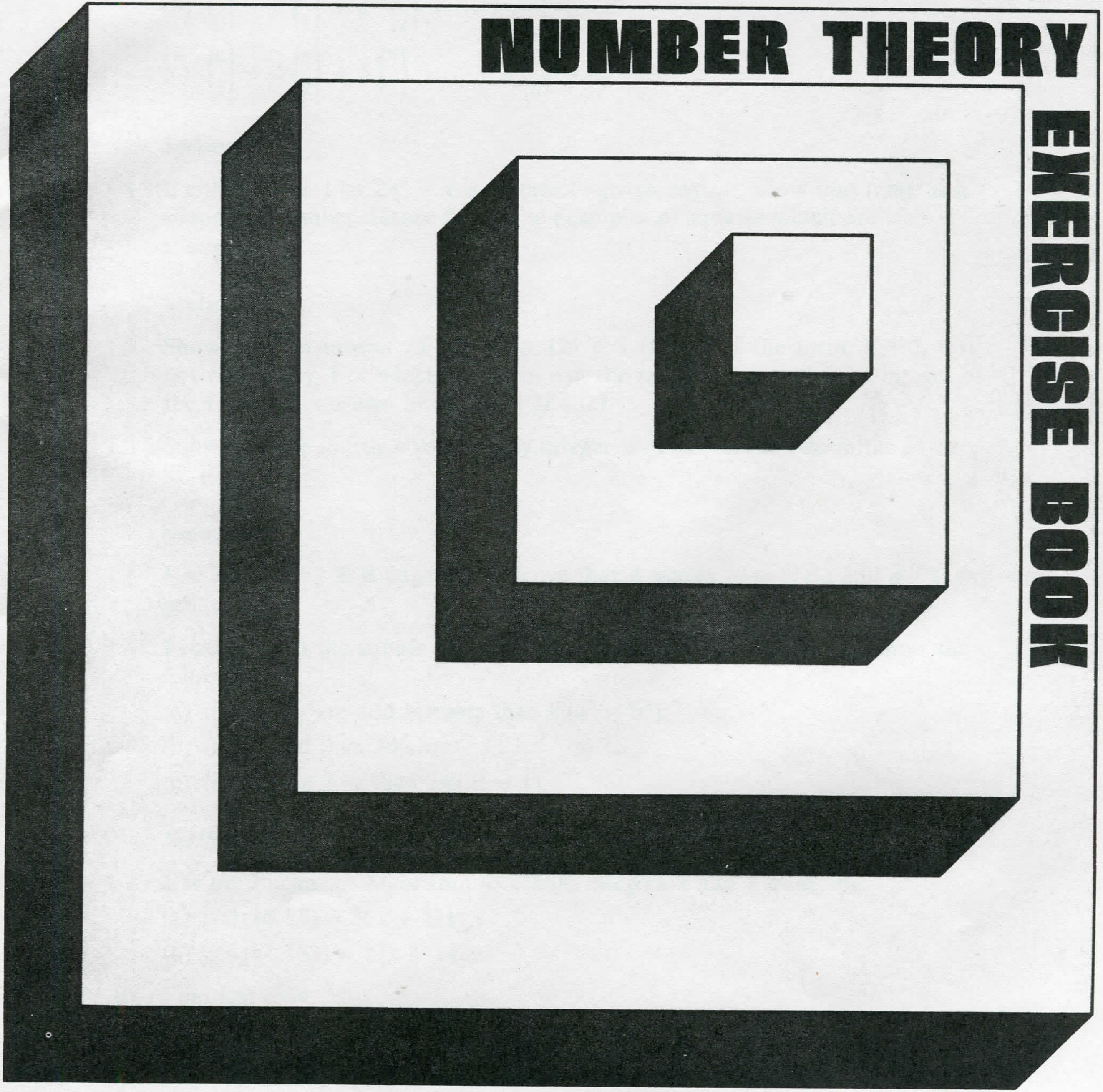
M335 NT EB

THE OPEN UNIVERSITY
Mathematics: A Third Level Course
M335 Studies in Pure Mathematics

STUDIES IN PURE MATHEMATICS

NUMBER THEORY

EXERCISE BOOK



Copyright © 1981 The Open University
1.4

SUP 06746 3

Unit 1

Drill Exercises

Section 1.1

1.1 Establish the following formulae by mathematical induction.

(a) $1 \cdot 2 + 2 \cdot 3 + \ldots + n(n+1) = \dfrac{n(n+1)(n+2)}{3}$, for all $n \geq 1$

(b) $1^2 + 3^2 + 5^2 + \ldots + (2n-1)^2 = \dfrac{n(4n^2-1)}{3}$, for all $n \geq 1$

1.2 For which positive integers n is it true that $n! > 6n^2$? Prove your result by mathematical induction.

Section 1.2

1.3 Use the Binomial Theorem to derive each of the following indentities.

(a) $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n} = 2^n$

(b) $\binom{n}{0} + 2\binom{n}{1} + 2^2\binom{n}{2} + \ldots + 2^n\binom{n}{n} = 3^n$

(c) $\binom{n}{1} + 2\binom{n}{2} + 3\binom{n}{3} + \ldots + n\binom{n}{n} = n2^{n-1}$

Section 1.3

1.4 If either $2n^2 + 1$ or $2n^2 - 1$ is a perfect square, say m^2, show that $(nm)^2$ is a triangular number. Hence find three examples of squares which are also triangular.

Section 1.4

1.5 Show that an integer of the form $12k + 8$ is also of the form $3l + 2$, but not conversely. For which values of r in the range $0 \leq r \leq 11$ is an integer of the form $12k + r$ also of the form $3l + 2$?

1.6 Show that the fourth power of any integer is of one of the two forms $8k$ or $8k + 1$.

Section 1.5

1.7 Use Theorem 2-4, **B** page 27, to prove that if $\gcd(a, b) = 1$, $c|a$ and $d|b$, then $\gcd(c, d) = 1$.

1.8 Recalling that the square of any odd integer is of the form $8k + 1$, show the following.

(a) If a and b are odd integers then $8|(a^2 - b^2)$.

(b) If a is odd then $24|a(a^2 - 1)$.

(c) If $2\nmid a$ and $3\nmid a$ then $24|(a^2 - 1)$.

Section 1.6

1.9 Use the Euclidean Algorithm to obtain integers x and y satisfying:

(a) $\gcd(36, 81) = 36x + 81y$;

(b) $\gcd(17, 143) = 17x + 143y$.

1.10 Find lcm (364, 390).

Section 1.7

1.11 Find all solutions in positive integers of the following Diophantine equations.

(a) $8x + 21y = 171$

(b) $158x - 57y = 7$

1.12 Using only 2p, 10p and 50p coins, in how many ways can exactly 100 coins be used in totalling £6?

Challenge Problems

1.13 Calculate $\binom{n+1}{1} + \binom{n+2}{2} + \binom{n+3}{3} + \ldots + \binom{n+k}{k}$.

1.14 Find all the ways in which the integer 1000 can be written as a sum of consecutive positive integers.

1.15

```
              x x 8 x x
       _________________
x x x ) x x x x x x x x
        x x x
        -----
          x x x x
            x x x
          -------
                x x x x
                x x x x
                =======
```

After spilling my coffee over the exact long division shown above, only the middle digit of the quotient is now legible. As it happens, enough information remains for you to reconstruct uniquely the long division.

Unit 2

Drill Exercises

Section 2.1

2.1 (a) If $p \neq 3$ is prime show that $3|p^2 + 2$.

(b) If $p \geq q \geq 5$ are primes show that $24|p^2 - q^2$.

2.2 (a) Show that if p and $8p - 1$ are both prime then $8p + 1$ is composite.

(b) Show that if p and $8p^2 + 1$ are both prime then $8p^2 - 1$ is also prime. [Hint: Can p and $8p^2 + 1$ both be prime?]

2.3 An integer is said to be *square-free* if it is not divisible by the square of any integer greater than 1. Prove that an integer $n > 1$ is square-free if and only if it is a product of distinct primes, and that every integer $n > 1$ is the product of a square-free integer and a perfect square.

2.4 Find the smallest integer which is divisible by both 2 and 3 and which is simultaneously both a square and a fifth power.

2.5 Show that if a, b and c are odd integers then the quadratic equation $ax^2 + bx + c = 0$ has no rational roots.

Section 2.2

2.6 Test 10261 for primality.

2.7 (a) Let p be the smallest prime factor of n, where n is composite. If $p > n^{1/3}$, prove that n/p is prime.

(b) If p and q are prime factors of n, each greater than $n^{1/4}$, is it necessarily the case that n/pq is prime?

2.8 Suppose there are only finitely many primes, say $p_1 = 2, p_2, p_3, \ldots, p_N$. Obtain a contradiction (thereby showing that there are infinitely many primes) by considering the number $2 + p_2p_3 \ldots p_N$.

Section 2.3

2.9 (a) For $n > 3$, show that n, $n + 2$ and $n + 4$ cannot all be prime.

(b) It can happen that n, $n + 2$, $n + 6$ and $n + 8$ are all prime. Use Table 2 of **B** (pages 358–67) to find six such prime quartets.

(c) If n, $n + 2$, $n + 6$, $n + 8$ is a prime quartet, what is the remainder when n is divided by 15?

2.10 Prove that if three prime numbers, all greater than 3, form an arithmetic progression, then the common difference of the progression is divisible by 6.

Section 2.4

2.11 Prove (a) if $2|u_n$ then $4|(u_{n+1}^2 - u_{n-1}^2)$;

(b) if $3|u_n$ then $9|u_{n+1}^3 - u_{n-1}^3)$.

2.12 Show that every eighth term of the Fibonacci sequence is divisible by 7.

Challenge Problems

2.13 Find all positive integers n which have the property that n is divisible by every integer r in the range $1 \leq r \leq \sqrt{n}$.

2.14 Prove that $n^4 + 4^n$ is composite for every integer $n \geq 2$.

2.15 Evaluate

(i) $\displaystyle\sum_{n=1}^{\infty} \frac{1}{u_n u_{n+2}}$, and

(ii) $\displaystyle\sum_{n=1}^{\infty} \frac{u_n}{10^n}$

where u_n is the nth Fibonacci number.

2.16 By considering the remainder sequence obtained by dividing each Fibonacci number by 10,000, show that amongst the first 10^8 Fibonacci numbers there must be one which terminates with four zeros.

Unit 3

Drill Exercises

Section 3.1

3.1 Determine the least positive residue and the least absolute residue of 1981 (a) modulo 7, (b) moldulo 17 and (c) modulo 101.

3.2 If $k \equiv 1 \pmod{12}$, then to what is $6k + 5$ congruent (a) modulo 12, (b) modulo 4?

3.3 (a) Give an example to show that $a^k \equiv b^k \pmod{n}$ need not imply that $a \equiv b \pmod{n}$.

(b) Give an example to show that $a^k \equiv b^k \pmod{n}$ and $k \equiv j \pmod{n}$ need not imply that $a^j \equiv b^j \pmod{n}$.

3.4 (a) What can the last digit of a fourth power be?

(b) Show that if $n \equiv 4 \pmod{5}$ then n cannot be written as a sum of three fourth powers.

3.5 Use the theory of congruences to verify that

$$89 | 2^{44} - 1 \quad \text{and} \quad 97 | 2^{48} - 1.$$

Section 3.2

3.6 (a) Without carrying out the multiplication, find the missing digit X in

$$1578 \cdot 34971 = 5518X238.$$

(b) What is the remainder when the product $89873569 \cdot 16641$ is divided by 11?

3.7 Show that the cubic equation $x^3 + 2x^2 + 4x + 2 = 0$ has no integer solutions.

3.8 N is a 10-digit number. A second integer M is formed using the same ten digits as in N, but in a different order, so that $N > M$. X is the sum of the digits of the number $N - M$. Show that the sum of the digits of X is 9.

Section 3.3

3.9 Solve the linear congruences.

(a) $8x \equiv 12 \pmod{60}$

(b) $21x \equiv 35 \pmod{47}$

(c) $6x \equiv 5 \pmod{41}$

(d) $5x \equiv 1 \pmod{93}$

3.10 Use the Chinese Remainder Theorem to find a positive integer n such that $3^2 | n$, $4^2 | n + 1$ and $5^2 | n + 2$.

3.11 Find the smallest odd integer $n > 3$ such that $3 | n$, $5 | n + 2$ and $7 | n + 4$.

Section 3.4

3.12 Using the identity $\mathbf{A}^{m+n} = \mathbf{A}^m \cdot \mathbf{A}^n$, where $\mathbf{A}$ is the matrix $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$, prove that

$$u_{m+n} = u_m u_{n-1} + u_{m+1} u_n, \quad \text{for } n \geq m > 1.$$

Deduce the identities

$$u_{2n-1} = u_n^2 + u_{n-1}^2 \quad \text{and} \quad u_{2n} = u_{n+1}^2 - u_{n-1}^2.$$

Challenge Problems

3.13 Let $A = 4444^{4444}$. If B is the sum of the digits of A, C is the sum of the digits of B, and D is the sum of the digits of C, what is D?

3.14 Find a positive integer such that one-half of it is a square, one-third of it is a cube and one-fifth of it is a fifth power.

3.15 Find the final digit of each of the numbers

$$(\ldots(((7^7)^7)^7)\ldots)^7 \quad \text{and} \quad 7^{\left(7^{\cdot^{\cdot^{\left(7^{\left(7^{7}\right)}\right)}}}\right)}$$

where, in both expressions, the integer 7 appears 1001 times. What are the final two digits of each?

Unit 4

Drill Exercises

Section 4.1

4.1 Use Fermat's method to factorize 65621.

Section 4.2

4.2 Find the least positive residues of $5^{12} \pmod{13}$, $5^{14} \pmod{13}$ and $1985^{14} \pmod{13}$.

4.3 What is the remainder when 7^{154} is divided by 155?

4.4 Show that $a^{1728} \equiv 1 \pmod{1729}$, for any integer a such that $\gcd(a, 1729) = 1$. [Note $1729 = 7 \cdot 13 \cdot 19$.]

4.5 If p and q are distinct primes, prove that $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

Section 4.3

4.6 If p is prime and a is any integer, prove that p divides both $a^p + (p-1)!\,a$ and $(p-1)!\,a^p + a$.

4.7 For p prime, prove that

$$(p-1)! \equiv p - 1 \pmod{1 + 2 + 3 + \ldots + (p-1)}.$$

Section 4.4

4.8 Show that $x^9 + 2x^8 + 6x + 5 \equiv (x^2 - 1)(x + 2) \pmod 7$ and hence solve

$$x^9 + 2x^8 + 6x + 5 \equiv 0 \pmod 7.$$

4.9 Find the quotient and remainder when $a(x)$ is divided by $b(x)$, where

(i) $a(x) = 2x^3 + 4x^2 - x + 1, \quad b(x) = x + 3;$

(ii) $a(x) = 3x^3 + 1, \quad b(x) = x^2 - x - 3.$

4.10 Solve the polynomial congruences.

(a) $x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \equiv 0 \pmod 5$

(b) $x^{12} - 1 \equiv 0 \pmod 7$

(c) $x^5 - x^3 \equiv 0 \pmod{11}$

(d) $x^5 + x^3 \equiv 0 \pmod{17}$

Challenge Problems

4.11 Prove that if $\gcd(n, 10) = 1$ then n^{101} terminates in the same three digits as does n.

4.12 Prove that $ab^p - ba^p$ is divisible by $6p$, where a and b are any integers and $p > 3$ is prime.

4.13 Prove that $\binom{2p}{p} \equiv 2 \pmod p$, where p is prime.

4.14 Verify that $\dfrac{13!}{5^2} \equiv 2!3! \pmod 5$.

Prove, more generally, that

$$\frac{n!}{p^k} \equiv (-1)^k k!\,(n-pk)! \pmod p,$$

where p is prime and $n = pk + r$, $0 \le r < p$. (That is, k is the quotient when n is divided by p.)

Unit 5

Drill Exercises

Section 5.1

5.1 Calculate $\tau(17640)$ and $\sigma(17640)$.

5.2 In 1644, Mersenne asked for a number with 60 divisors. Find the smallest one.

5.3 For any integer $n > 1$ prove that $\tau(n) < 2\sqrt{n}$ and, if n is composite, that $\sigma(n) > n + \sqrt{n}$.

5.4 Prove that if $f(n)$ is a multiplicative function then so too is $g(n) = \frac{1}{n} f(n)$.

5.5 Show that if $n > 6$ is an even perfect number then $n \equiv 1 \pmod 9$. [Hint: $n = 2^{r-1}(2^r - 1)$, where $2^r - 1$ is prime.]

Section 5.2

5.6 Find the exponent of the highest power of prime p dividing
(a) the product $2\cdot 4\cdot 6\cdot\ldots\cdot(2n)$ of the first n even integers;
(b) the product $1\cdot 3\cdot 5\cdot\ldots\cdot(2n-1)$ of the first n odd integers.

Section 5.3

5.7 Calculate $\phi(520)$ and $\phi(546)$.

5.8 If p is prime, show that
(a) $\sigma(p) = \tau(p) + \phi(p)$;
(b) $\sigma(p) + \phi(p) = p\tau(p)$.

5.9 Show that $\gcd(m, n) = 2$ implies that $\phi(mn) = 2\phi(m)\phi(n)$.

5.10 Show that if $n - 1$ and $n + 1$ are both primes, where $n > 4$, then $\phi(n) \le n/3$.

Section 5.4

5.11 Find the remainder when 13^{83} is divided by 40.

5.12 Find the multiplicative inverses of 5 and 25 modulo 28, and hence solve the linear congruences

$$5x \equiv 11 \pmod{28} \quad \text{and} \quad 25x \equiv 11 \pmod{28}.$$

5.13 If p and q are distinct primes, prove that

$$p^q + q^p \equiv p + q \pmod{pq}.$$

Challenge Problems

5.14 Prove that n is prime if and only if

$$\phi(n) + \sigma(n) = n\tau(n).$$

5.15 Prove that

(a) $\tau(1) + \tau(2) + \ldots + \tau(n) = \left[\frac{n}{1}\right] + \left[\frac{n}{2}\right] + \ldots + \left[\frac{n}{n}\right]$,

(b) $\sigma(1) + \sigma(2) + \ldots + \sigma(n) = \left[\frac{n}{1}\right] + 2\left[\frac{n}{2}\right] + \ldots + n\left[\frac{n}{n}\right]$,

where [ ] denotes the greatest integer function.

5.16 Let n be an odd positive integer. Prove that there are $\tau(n)$ ways of expressing n as a sum of consecutive positive integers. (For example, the $\tau(15) = 4$ ways of expressing 15 as a sum of consecutive integers are

$$1 + 2 + 3 + 4 + 5; \quad 4 + 5 + 6; \quad 7 + 8; \quad 15.)$$

Show that no number of the form 2^k can be written as a sum of two or more consecutive positive integers.

Unit 6

Drill Exercises

Section 6.1

6.1 For which integer values of c does the congruence $2x^2 - 5x + c \equiv 0 \pmod{13}$ have solutions? Solve the congruence for the case $c = 1$. [Hint: The information in Example 9-1 on **B** page 186 may prove helpful.]

6.2 Use Euler's Criterion to determine whether or not 3 is a quadratic residue of (a) 17, (b) 19.

6.3 If $n > 2$ and $\gcd(a, n) = 1$ then a is called a quadratic residue of n if $x^2 \equiv a \pmod{n}$ for some integer x. Prove that if a is a quadratic residue of $n > 2$ then $a^{\phi(n)/2} \equiv 1 \pmod{n}$. Show that the converse of this result is false, by finding relatively prime integers a and n for which $a^{\phi(n)/2} \equiv 1 \pmod{n}$ but for which the congruence $x^2 \equiv a \pmod{n}$ has no solutions.

Section 6.2

6.4 Evaluate the Legendre symbols

$$(18/19),\ (45/19) \text{ and } (2/19).$$

6.5 Find all quadratic residues of 29.

6.6 If p is an odd prime and $\gcd(a, p) = 1$, show that

$$(p - 1)! \equiv -(a/p)a^{(p-1)/2} \pmod{p}.$$

Section 6.3

6.7 Use Gauss' Lemma to evaluate the Legendre symbols

$$(7/13),\ (11/23) \text{ and } (3/29).$$

6.8 Show that 2 is a quadratic residue of

(a) every prime of the form $4^n + 1$, for $n > 1$,

(b) every Mersenne prime $M_p = 2^p - 1$, except $M_2 = 3$, and

(c) every Fermat prime $2^{2^n} + 1$, for $n > 1$.

For each of these primes decide whether or not -2 is a quadratic residue.

Section 6.4

6.9 Calculate $(35/71)$, $(139/149)$ and $(1234/4567)$.

6.10 Which of the following congruences have solutions?

(a) $2x^2 + x + 1 \equiv 0 \pmod{29}$

(b) $2x^2 + 3x - 7 \equiv 0 \pmod{101}$

6.11 (a) If p and $q = 10p + 3$ are odd primes, show that $(p/q) = (3/p)$.

(b) If p and $q = 10p + 1$ are odd primes, show that $(p/q) = (-1/p)$.

6.12 Show that 3 is a quadratic nonresidue of each of the primes listed in Problem 6.8.

Challenge Problems

6.13 Prove that there are infinitely many primes of the forms (a) $5k + 4$, (b) $8k + 5$.

6.14 For $p > 5$, prove that there are consecutive integers which are both quadratic residues of p, and that there are consecutive integers which are both quadratic nonresidues of p.

6.15 Evaluate, for p an odd prime,

$$((1 \cdot 2)/p) + ((2 \cdot 3)/p) + \ldots + ((p-2)(p-1)/p).$$

Unit 7

Drill Exercises

Section 7.1

7.1 Express each of the rational numbers below as a finite continued fraction with an even number of partial denominators.

(a) $\dfrac{39}{14}$, (b) $\dfrac{-41}{37}$, (c) $\dfrac{117}{304}$.

7.2 Compute the convergents of the following continued fractions:

(a) $[2; 3, 1, 7]$, (b) $[0; 5, 4, 3, 2, 1]$, (c) $[-3; 1, 1, 1, 1, 19]$.

7.3 Find the simple continued fraction representations of 3.1416 and 2.718.

7.4 Use the method of continued fractions to determine the general solution of each of the following linear Diophantine equations.

(a) $13x + 24y = 1$

(b) $86x + 97y = 8$

(c) $15x - 43y = 7$

7.5 Verify Theorem 13-8, **B** pages 310 and 311, for the continued fraction $[2; 4, 4, 4, 4, 4, 4, 4]$.

Section 7.2

7.6 Evaluate the periodic continued fractions

$$[\overline{5;3,1}],\quad [\overline{3;1,5}],\quad [0;1,\overline{5,3,1}] \quad \text{and} \quad [-3;1,1,\overline{3,1,5}].$$

Section 7.3

7.7 Determine the infinite continued fraction representation of the following irrationals:

(a) $\sqrt{18}$, (b) $\dfrac{1+\sqrt{13}}{2}$, (c) $\dfrac{4+\sqrt{21}}{5}$.

7.8 Euler showed that the continued fraction of the irrational number $\dfrac{e^{2/k}-1}{e^{2/k}+1}$ is $[0;k,3k,5k,7k,\ldots]$, for any positive integer k. Use this information to find values for $\dfrac{e-1}{e+1}$ and $\dfrac{e^2-1}{e^2+1}$ which are correct to five decimal places.

Section 7.4

7.9 Let $\alpha = [\overline{1;3,4,1}]$ and $\beta = [\overline{1;4,3,1}]$. Verify that the algebraic conjugate of α is $-1/\beta$.

7.10 One of the irrational numbers below has a purely periodic continued fraction. Decide which one it is and then find its continued fraction.

$$3+3\sqrt{2},\quad \frac{3+\sqrt{15}}{6},\quad \frac{-10-4\sqrt{5}}{3}.$$

Section 7.5

7.11 With the usual notation for the convergents to the irrational number x, suppose $\left|x-\dfrac{a}{b}\right| < \left|x-\dfrac{p_n}{q_n}\right|$, where $0 < b < q_{n+1}$. Prove that $aq_n - bp_n = \pm 1$.

7.12 Without calculating the continued fraction, show that 17/16 is a convergent of $\dfrac{2+\sqrt{11}}{5}$.

Challenge Problems

7.13 Let $\alpha = [a_0; a_1, a_2, a_3, \ldots]$.

(i) Find the continued fraction of $-\alpha$.

(ii) Show that, provided a_1 is even, the continued fraction of 2α satisfies

$$2[a_0;a_1,a_2,a_3,\ldots] = [2a_0;\frac{a_1}{2},2[a_2;a_3,a_4,\ldots]] \qquad (*)$$

and deduce that, provided all the odd numbered partial denominators are even,

$$2[a_0;a_1,a_2,a_3,\ldots] = [2a_0;\frac{a_1}{2},2a_2,\frac{a_3}{2},2a_4,\frac{a_5}{2},\ldots].$$

(iii) Find a formula corresponding to $(*)$ for the case when a_1 is odd.

7.14 Let $\mathbf{A}_n = \begin{pmatrix} 0 & 1 \\ 1 & a_n \end{pmatrix}$ and $\mathbf{M}_n = \begin{pmatrix} q_{n-2} & p_{n-2} \\ q_{n-1} & p_{n-1} \end{pmatrix}$, where $\{p_n/q_n\}$, $n \geqslant 0$, are the convergents of $[a_0;a_1,a_2,a_3,\ldots]$. Show that

(i) $\mathbf{M}_{n+1} = \mathbf{A}_n\mathbf{M}_n, \quad n \geqslant 2$,

(ii) $\mathbf{M}_{n+1} = \mathbf{A}_n\mathbf{A}_{n-1}\ldots\mathbf{A}_2\mathbf{A}_1\mathbf{A}_0$.

By considering the determinant of $\mathbf{M}_n$, deduce the formula

(iii) $p_n q_{n-1} - q_n p_{n-1} = (-1)^{n-1}$,

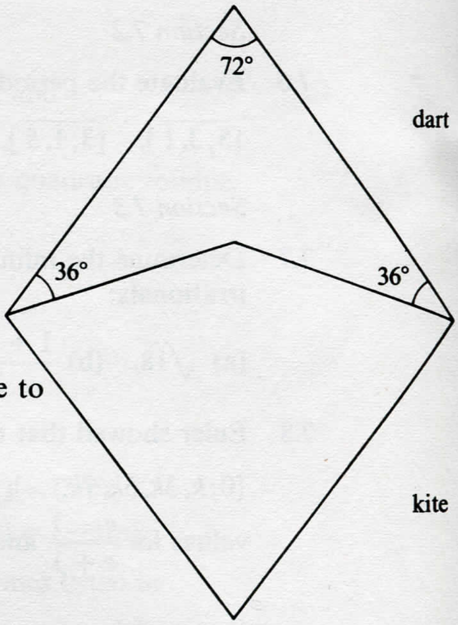
and from $\mathbf{M}_n$ and its transpose deduce

(iv) $\dfrac{p_n}{p_{n-1}} = [a_n; a_{n-1}, \ldots, a_1, a_0]$

and

(v) $\dfrac{q_n}{q_{n-1}} = [a_n; a_{n-1}, \ldots, a_1]$.

7.15 A rhombus with acute angle 72° is divided into dart and kite shaped figures as shown. Prove that the ratio of the areas, kite to dart, is the golden ratio.



Unit 8

Drill Exercises

Section 8.1

8.1 Find three positive solutions of
(a) $x^2 - 24y^2 = 1$, (b) $x^2 - 37y^2 = 1$.

8.2 Establish that if x_0, y_0 is a solution of $x^2 - dy^2 = -1$, then $x = 2x_0^2 + 1$, $y = 2x_0 y_0$ satisfies $x^2 - dy^2 = 1$. Use this fact to find a solution of $x^2 - 74y^2 = 1$. [Hint: $\sqrt{74} = [8; \overline{1, 1, 1, 1, 16}]$.]

8.3 Find three positive solutions of $x^2 + 2xy - 2y^2 = 1$.

Section 8.2

8.4 If x, y, z is a primitive Pythagorean triple prove that $x + y$ and $x - y$ are congruent modulo 8 to either 1 or 7.

8.5 Find all Pythagorean triangles (i.e. right-angled triangles with integer sides) which have the property that their area is equal to their perimeter.

Section 8.3

8.6 Does $x^8 + y^8 = z^4$ have any positive solutions?

8.7 Use the method of infinite descent to show that $x^3 + py^3 = p^2z^3$ has no positive solutions, where p is any prime.

8.8 Show that $x^2 + y^2 = x^2y^2$ has no positive solutions.

Section 8.4

8.9 If m and n are sums of two squares and $m|n$, is it true that $\dfrac{n}{m}$ is a sum of two squares? Prove, or give a counterexample.

8.10 Find the three smallest integers greater than 1000 which cannot be expressed as a sum of three squares.

Challenge Problems

8.11 Find eight triangular squares (i.e. squares which are also triangular numbers).

8.12 Show that 169 can be expressed as a sum of one, two, three and four non-zero squares. Hence show that every integer greater than 169 is a sum of five *non-zero* squares.

Which positive integers cannot be expressed as a sum of five non-zero squares?

8.13 Consider the following three sets of numbers: {1, 15, 22, 50, 57, 71}, {2, 11, 27, 45, 61, 70} and {5, 6, 35, 37, 66, 67}. The sum of each set is 216, and the sum of the squares of each set is 11500. Nothing marvellous so far, but it is mildly surprising to discover that the sums of the cubes of each set are also the same, 682128. But things really get interesting when we find that the sums of the fourth powers are each 42502564, and the sums of the fifth powers are also the same, namely 2724334416.

Sets of numbers with curious properties like this are called *multigrades*, and many fascinating examples are known. As a first challenge, try to find two disjoint sets of three positive integers for which the sums and the sums of the squares are equal.

Solutions

1.1 (a) The formula is true for $n = 1$, since $1 \cdot 2 = \dfrac{1 \cdot 2 \cdot 3}{3}$.

Assume the formula is true for $n = k$, that is,

$$1 \cdot 2 + 2 \cdot 3 + \ldots + k(k+1) = \tfrac{1}{3}k(k+1)(k+2).$$

Then, adding $(k+1)(k+2)$ to both sides,

$$\begin{aligned} 1 \cdot 2 + \ldots + k(k+1) + (k+1)(k+2) &= \tfrac{1}{3}k\,(k+1)(k+2) + (k+1)(k+2) \\ &= (k+1)(k+2)(\tfrac{1}{3}k + 1) \\ &= \tfrac{1}{3}(k+1)(k+2)(k+3), \end{aligned}$$

establishing the truth of the formula for $n = k + 1$. By the First Principle of Finite Induction, the formula is true for all $n \geq 1$.

(b) The formula is true for $n = 1$, since $1^2 = \dfrac{1(4 \cdot 1^2 - 1)}{3}$.

Assume the formula is true for $n = k$, that is,

$$1^2 + 3^2 + \ldots + (2k-1)^2 = \tfrac{1}{3}k(4k^2 - 1).$$

Then, adding $(2k+1)^2$ to both sides,

$$\begin{aligned} 1^2 + 3^2 + \ldots + (2k-1)^2 + (2k+1)^2 &= \tfrac{1}{3}k(4k^2 - 1) + (2k+1)^2 \\ &= \tfrac{1}{3}k(2k-1)(2k+1) + (2k+1)^2 \\ &= \tfrac{1}{3}(2k+1)\,[k(2k-1) + 6k + 3] \\ &= \tfrac{1}{3}(2k+1)(2k^2 + 5k + 3) \\ &= \tfrac{1}{3}(2k+1)(2k+3)(k+1) \\ &= \tfrac{1}{3}(k+1)(4k^2 + 8k + 3) \\ &= \tfrac{1}{3}(k+1)(4(k+1)^2 - 1), \end{aligned}$$

establishing the truth of the formula for $n = k + 1$. By the First Principle Finite Induction, the formula is true for all $n \geq 1$.

1.2 $n!$ increases more rapidly than $6n^2$, and $n!$ exceeds $6n^2$ for the first time when $n = 6$. So we conjecture that $n! > 6n^2$ for all $n \geq 6$, and prove it by mathematical induction.

$6! = 720 > 6 \cdot 6^2 = 216$, so the conjecture is true for $n = 6$. Assume that $k! > 6k^2$, for some $k \geq 6$. Then, multiplying both sides by $k + 1$,

$$(k+1)! > 6k^2\,(k+1).$$

If we can establish that $k^2 \geq k + 1$ it will follow that $(k+1)! > 6(k+1)^2$, completing the induction step. But this is easily seen since, for $k \geq 6$,

$$k^2 \geq 6k > 2k = k + k > k + 1.$$

The conjecture is true for all $n \geq 6$ by the First Principle of Finite Induction.

1.3 Binomial Theorem:

$$(a+b)^n = \binom{n}{0} a^n + \binom{n}{1} a^{n-1}b + \ldots + \binom{n}{r} a^{n-r}b^r + \ldots + \binom{n}{n} b^n.$$

(a) Put $a = b = 1$. Then $2^n = \binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{n}$.

(b) Put $a = 1$, $b = 2$. Then $3^n = \binom{n}{0} + 2\binom{n}{1} + 2^2\binom{n}{2} + \ldots + 2^n\binom{n}{n}$.

(c) $\binom{n}{1} + 2\binom{n}{2} + 3\binom{n}{3} + \ldots + n\binom{n}{n} = \sum_{r=1}^{n} r\binom{n}{r}$.

Now $r\binom{n}{r} = \dfrac{r \cdot n!}{r!(n-r)!} = \dfrac{n!}{(r-1)!\,(n-r)!} = n \cdot \dfrac{(n-1)!}{(r-1)!\,(n-r)!} = n\binom{n-1}{r-1}$.

$$\text{So } \binom{n}{1} + 2\binom{n}{2} + \ldots + n\binom{n}{n} = \sum_{r=1}^{n} r\binom{n}{r} = \sum_{r=1}^{n} n\binom{n-1}{r-1}$$

$$= n\sum_{r=0}^{n-1}\binom{n-1}{r} = n2^{n-1} \qquad \text{by (a).}$$

1.4 If $m^2 = 2n^2 \pm 1$, then $(mn)^2 = n^2(2n^2 \pm 1) = \frac{1}{2}2n^2(2n^2 \pm 1)$, and the latter is a triangular number since $2n^2 \pm 1$ is consecutive with $2n^2$.

The first three square values for $2n^2 \pm 1$ are

$n = 1$, $2n^2 - 1 = 1$, giving triangular square $n^2(2n^2 - 1) = 1$;

$n = 2$, $2n^2 + 1 = 9$, giving triangular square $n^2(2n^2 + 1) = 36$;

$n = 5$, $2n^2 - 1 = 49$, giving triangular square $n^2(2n^2 - 1) = 1225$.

(If you overlooked $n = 1$ the next is $12^2(2 \cdot 12^2 + 1) = 41616$.)

1.5 $12k + 8 = 3(4k + 2) + 2 = 3l + 2$, where $l = 4k + 2$ is an integer. The number 5 is of the form $3k + 2$ but not of the form $12k + 8$ (since the remainder on division by 12 is 5, not 8).

Suppose that $12k + r\,(0 \leq r \leq 11)$ is also of the form $3k + 2$. This means that the remainder on dividing $12k + r$ by 3 is 2. But $3|12k$, and so the remainder on dividing r by 3 is 2. The values of r with this property are $r = 2, 5, 8$ and 11.

1.6 The square of any odd integer is of the form $8k + 1$ (see **B** page 22). Squaring again,

$$(8k + 1)^2 = 8(8k^2 + 2k) + 1 = 8k' + 1,$$

showing that the fourth power of any odd integer is of the form $8k + 1$.

Any even integer is of the form $n = 2r$, r an integer, so

$$n^4 = (2r)^4 = 16r^4 = 8(2r^4) = 8k.$$

1.7 $c|a$ and $d|b$ means that there exist integers k and l such that $a = kc$ and $b = ld$. Since $\gcd(a, b) = 1$, Theorem 2-4 tells us that $ax + by = 1$, for some integers x and y. Therefore

$$kcx + ldy = c(kx) + d(ly) = 1,$$

from which Theorem 2-4 confirms that $\gcd(c, d) = 1$.

1.8 (a) $a^2 = 8k + 1$ and $b^2 = 8l + 1$, for some integers k and l. Therefore $a^2 - b^2 = 8(k - l)$, showing that $8|(a^2 - b^2)$.

(b) We shall show that $8|a(a^2 - 1)$ and $3|a(a^2 - 1)$. The result then follows from Corollary 2 (**B** page 28), since $\gcd(3, 8) = 1$. Since a is odd, $a^2 = 8k + 1$, from which it follows that $8|a^2 - 1$. Therefore $8|a(a^2 - 1)$.

a is of one of the three forms $3k$, $3k + 1$ or $3k + 2$. If $a = 3k$ then $3|a$ and so $3|a(a^2 - 1)$. If $a = 3k + 1$ then $a^2 - 1 = 9k^2 + 6k = 3(3k^2 + 2k)$, and if $a = 3k + 2$ then $a^2 - 1 = 9k^2 + 12k + 3 = 3(3k^2 + 4k + 1)$. For each of these cases $3|a^2 - 1$, and so in all cases $3|a(a^2 - 1)$.

We conclude that $24|a(a^2 - 1)$, for any odd integer a.

(c) $2\nmid a$ means that a is odd and so $8|a^2 - 1$. $3\nmid a$ means that a is of one of the forms $3k + 1$ or $3k + 2$, and, as shown in (b), $3|a^2 - 1$. By Corollary 2, $24|a^2 - 1$.

1.9 (a)
$$\left.\begin{aligned} 81 &= 2\cdot 36 + 9\\ 36 &= 4\cdot 9\end{aligned}\right\}\Longrightarrow\begin{aligned}&\gcd(36, 81) = 9 = 81 - 2\cdot 36\\ &\text{So } x = -2,\ y = 1.\end{aligned}$$

(b)
$$\left.\begin{aligned} 143 &= 8\cdot 17 + 7\\ 17 &= 2\cdot 7 + 3\\ 7 &= 2\cdot 3 + 1\\ 3 &= 3\cdot 1\end{aligned}\right\}\Longrightarrow\begin{aligned}\gcd(17, 143) = 1 &= 7 - 2\cdot 3\\ &= 7 - 2\cdot(17 - 2\cdot 7)\\ &= 5\cdot(143 - 8.17) - 2.17\\ &= 5\cdot 143 - 42\cdot 17\end{aligned}$$

So $x = -42$, $y = 5$.

$7 + 4\cdot 7 - 2\cdot 17$
$= 5\cdot 7 - 2\cdot 17$
~~$143 - 8\cdot 17 + 4\cdot 7 - 2\cdot 1$~~

1.10 $390 = 1\cdot 364 + 26$

$364 = 14\cdot 26 + 0$

So $\gcd(364, 390) = 26$ and $\operatorname{lcm}(364, 390) = \dfrac{364\cdot 390}{26} = 5460$.

1.11 (a) $8\cdot 8 + 21\cdot(-3) = 1$ (by the Euclidean Algorithm or inspection), and so $8\cdot(8\cdot 171) + 21\cdot(-3\cdot 171) = 171$, giving one solution $x_0 = 8\cdot 171 = 1368$, $y_0 = -3\cdot 171 = -513$. The general solution is gcd(8, 21)

$$\{x = 1368 - 21t,\ y = -513 + 8t\colon t \text{ any integer}\}.$$

For positive solutions, we requre $1368 > 21t$ and $513 < 8t$. The only value of t satisfying both conditions is $t = 65$, giving the unique positive solution $x = 3$, $y = 7$.

$158x \mp 57y = 7$

(b)
$$\begin{aligned} 158 &= 2\cdot 57 + 44 & \gcd(158, 57) = 1 &= 3 - 2\\ 57 &= 1\cdot 44 + 13 & &= 3 - (5 - 3)\\ 44 &= 3\cdot 13 + 5 & &= 2\cdot(13 - 2\cdot 5) - 5\\ 13 &= 2\cdot 5 + 3 & &= -5\cdot(44 - 3\cdot 13) + 2\cdot 13\\ 5 &= 1\cdot 3 + 2 & &= 17\cdot(57 - 44) - 5\cdot 44\\ 3 &= 1\cdot 2 + 1 & &= -22\cdot(158 - 2\cdot 57) + 17\cdot 57\\ 2 &= 2\cdot 1 & &= 158\cdot(-22) + 57\cdot 61\end{aligned}$$

$$\begin{array}{r} 171\\ -154\\ \hline 17\end{array}\qquad\begin{array}{r} 474\\ 427\\ \hline 47\end{array}$$

Therefore $7 = 158\cdot(-154) + 57\cdot 427$, giving $x_0 = -154$ and $y_0 = -427$ as one solution of $158x - 57y = 7$. The general solution is

$$\{x = -154 + 57t,\ y = -427 + 158t\colon t \text{ any integer}\}.$$

For x and y to be both positive requires $t \geq 3$. When $t = 3$ the least positive solution is $x = 17$, $y = 47$, and all positive solutions are given by $x = 17 + 57t$, $y = 47 + 158t$, for any integer $t \geq 0$.

1.12 Suppose that the number of 2p, 10p and 50p coins used are x, y and z respectively. Then $x + y + z = 100$ and, for a total of £6, $2x + 10y + 50z = 600$. Eliminating x from this pair of equations gives

$$8y + 48z = 400 \quad \text{or} \quad y + 6z = 50.$$

One solution of this linear Diophantine equation is $y_0 = 50$, $z_0 = 0$ giving general solution

$$\{y = 50 - 6t,\ z = t\text{: } t \text{ any integer}\}.$$

Substituting back into either of the original equations gives $x = 50 + 5t$, so the complete solution is

$$\{x = 50 + 5t,\ y = 50 - 6t,\ z = t\text{: } t \text{ any integer}\}.$$

Of course, we are interested only in non-negative solutions. $t \geq 0$ is needed to ensure that z is non-negative (and this also ensures that x is non-negative), and $t \leq 8$ is needed for $y \geq 0$. There are therefore *nine* solutions, namely those given by $t = 0, 1, 2, 3, 4, 5, 6, 7$ and 8.

2.1 (a) If $p \neq 3$ is prime then p is of one of the forms $3k + 1$ or $3k + 2$ (since $3k$ is composite for $k > 1$). As in Problem 1.8(b), it now follows that $p^2 = 3r + 1$, for some integer r. But then $p^2 + 2 = 3(r + 1)$ is divisible by 3.

(b) Since p is odd, p^2 is of the form $8k + 1$ and, since $p \neq 3$, p^2 is of the form $3r + 1$. Therefore $p^2 - 1$ is divisible by both 8 and 3, and as $\gcd(8, 3) = 1$, $p^2 - 1$ is divisible by 24. So $p^2 = 24s + 1$, for some integer s. [This is the result of Problem 1.8(c).]

Similarly, $q^2 = 24t + 1$, for some integer t, and so $p^2 - q^2 = 24(s - t)$ is divisible by 24.

2.2 (a) Either $p = 3$, or p is of one of the forms $3k + 1$ or $3k + 2$.

$p = 3 \Rightarrow 8p - 1 = 23$ and $8p + 1 = 25$ is composite.

$p = 3k + 1 \Rightarrow 8p + 1 = 24k + 9 = 3(8k + 3)$ is composite (regardless of whether or not $8p - 1$ is prime).

$p = 3k + 2 \Rightarrow 8p - 1 = 24k + 15 = 3(8k + 5)$ is composite.

(b) If $p \neq 3$ then $p^2 = 3k + 1$, for some integer k. But then $8p^2 + 1 = 24k + 9 = 3(8k + 3)$ is not prime.

The only occasion on which p and $8p^2 + 1$ are both prime is when $p = 3$ and $8p^2 + 1 = 73$. In this case $8p^2 - 1 = 71$ is also prime.

2.3 Let n have prime factorization $p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$. If n is square-free then $p_i^2 \nmid n$ and so $k_i = 1$, for $i = 1, 2, \dots, r$, and n is a product of distinct primes. On the other hand, if $n = p_1 p_2 \dots p_r$ then the divisors of n are the numbers $p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$, where each $k_i = 0$ or 1. The only divisor of n which is a square (all exponents even) is 1, and so n is square-free.

In the prime factorization of any integer n, each exponent is either even or odd. Listing the primes with even exponent first,

$$n = p_1^{2k_1} p_2^{2k_2} \dots p_r^{2k_r} q_1^{2l_1 + 1} \dots q_s^{2l_s + 1},$$

where each $k_i \geq 1$ and each $l_j \geq 0$. But then

$$n = (p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} q_1^{l_1} \dots q_s^{l_s})^2\, q_1 q_2 \dots q_s$$

is a perfect square times a square-free integer. [Note that either the square or the square-free part might be non-existent, a possibility catered for by the fact that 1 is both square-free and a square.]

2.4 Let the integer be n. Since $2|n$ and $3|n$, $n = 2^a \cdot 3^b \cdot N$ for some positive integers a, b and N, with $\gcd(6, N) = 1$.

To be a square, the exponents a and b must both be even. To be a fifth power, a and b must both be multiples of 5. Therefore $n = 2^{10c} \cdot 3^{10d} \cdot N$, where N is a tenth power. The smallest such integer occurs when $c = d = N = 1$, and is 6^{10}.

2.5 Suppose $ax^2 + bx + c = 0$ has root $x = m/n$ where $\gcd(m, n) = 1$. Then $am^2 + bmn + cn^2 = 0$. Since a, b and c are given to be odd and one (or both) of m or n is odd, it is seen that $am^2 + bmn + cn^2$ is always odd, and so cannot possibly be equal to 0.

Alternatively: The quadratic has rational roots precisely when $b^2 - 4ac$ is a perfect square. (By SAQ 7, if $\sqrt{b^2 - 4ac}$ is rational then it is an integer.) Putting $a = 2r + 1$, $b = 2s + 1$ and $c = 2t + 1$ we get

$$b^2 - 4ac = 8\left(\frac{s(s+1)}{2} - 2rt - r - t\right) - 3.$$

But we have seen (**B** page 22) that no integer of the form $8k - 3$ can be a perfect square. Hence the result.

2.6 We need to test 10261 for divisibility by each of the primes up to and including 101, since $101^2 < 10261 < 102^2$. In fact, we meet with success at the prime 31: $10261 = 31 \cdot 331$.

COMMENT To test divisibility of 10261 by various primes without the aid of a calculator there are numerous shortcuts available. For example:

If 10261 is divisible by 13 then so too is $10261 + 39 = 103 \cdot 100$. But this is false since $13 \nmid 103$ and $13 \nmid 100$.

If 10261 is divisible by 11 then so too is $10261 - 11 = 250 \cdot 41$, and if 10261 is divisible by 61 then so too is $10261 - 61 = 102 \cdot 100$, both of which are clearly false.

On the other hand, 10261 is divisible by 31 if and only if $10261 - 31$ is divisible by 31. Now $10261 - 31 = 1023 \cdot 10 = 31 \cdot 33 \cdot 10$, so this is the case.

2.7 (a) Let $n = pN$ where $p > n^{1/3}$ is the smallest prime factor of n. Then $N = n/p < n^{2/3}$. If N is composite then N has a prime factor $q \leq \sqrt{N}$. But such a q is a prime factor of n (since N divides n) and $q \leq \sqrt{N} < n^{1/3}$ contradicts the minimality of p. We conclude that N is prime.

(b) NO. Consider $n = 2 \cdot 3 \cdot 5 \cdot 7$. 5 and 7 are each greater than $n^{1/4}$ but $n/5 \cdot 7 = 6$, which is composite.

2.8 Suppose there are only finitely many primes $p_1 = 2, p_2, p_3, \ldots, p_N$ and consider the number $M = 2 + p_2 p_3 \ldots p_N$. M is odd and so must be divisible by an odd prime p_r, for some $2 \leq r \leq N$. But $p_r | p_2 p_3 \ldots p_r \ldots p_N$ and so $p_r | (M - p_2 p_3 \ldots p_N)$. That is $p_r | 2$, which is a contradiction.

2.9 (a) n is of one of the forms $3k$, $3k + 1$ or $3k + 2$.

$n = 3k \implies n$ composite (for $k > 1$).

$n = 3k + 1 \implies n + 2 = 3(k + 1)$ is composite.

$n = 3k + 2 \implies n + 4 = 3(k + 2)$ is composite.

(b) 11, 13, 17, 19; 101, 103, 107, 109; 191, 193, 197, 199; 821, 823, 827, 829; 1481, 1483, 1487, 1489; 1871, 1873, 1877, 1879.

COMMENT Prime quartets are of the form $10k + 1$, $10k + 3$, $10k + 7$ and $10k + 9$, since the missing odd number must be a multiple of 5. There is, however, the one exceptional prime quartet: 5, 7, 11, 13. It is not known whether or not there are infinitely many prime quartets.

(c) For the quartet 5, 7, 11, 13, the answer is 5. Otherwise, the missing number $n + 4$ must be divisible by 3 (from part (a)), and similarly must be divisible by 5 (for otherwise one of the alleged primes is a multiple of 5). Therefore $n + 4$ is a multiple of 15, and the remainder on dividing n by 15 is 11.

2.10 Let the three primes be a, $a + d$ and $a + 2d$, where $a > 3$ and $d \geq 1$. Observe immediately that d must be even, for if d is odd the terms are alternately odd and even, and an even term cannot be prime. So to establish that $6|d$ we need to show that $3|d$ (Corollary 2, **B** page 28).

Suppose to the contrary that $3\not|d$, so that d is of one of the forms $3k + 1$ or $3k + 2$. As a is a prime greater than 3 it is also of one of these two forms. In each case either $a + d$ or $a + 2d$ is divisible by 3:

a	d	Divisible by 3
$3r + 1$	$3k + 1$	$a + 2d = 3(r + 2k + 1)$
$3r + 1$	$3k + 2$	$a + d = 3(r + k + 1)$
$3r + 2$	$3k + 1$	$a + d = 3(r + k + 1)$
$3r + 2$	$3k + 2$	$a + 2d = 3(r + 2k + 2)$

This gives a contradiction, and so $3|d$ as required.

2.11 (a)
$$u^2_{n+1} - u^2_{n-1} = (u_{n+1} - u_{n-1})(u_{n+1} + u_{n-1})$$
$$= u_n(u_n + 2u_{n-1}) \qquad (\text{using } u_{n+1} = u_n + u_{n-1}).$$

Now if $2|u_n$ then $2|(u_n + 2u_{n-1})$ and so $4|u^2_{n+1} - u^2_{n-1}$.

(b)
$$u^3_{n+1} - u^3_{n-1} = (u_{n+1} - u_{n-1})(u^2_{n+1} + u_{n-1}u_{n+1} + u^2_{n-1})$$
$$= u_n[(u_n + u_{n-1})^2 + u_{n-1}(u_n + u_{n-1}) + u^2_{n-1}]$$
$$= u_n(u^2_n + 3u_nu_{n-1} + 3u^2_{n-1}).$$

Now if $3|u_n$ then $3|(u^2_n + 3u_nu_{n-1} + 3u^2_{n-1})$ and $9|u^3_{n+1} - u^3_{n-1}$.

2.12 Replacing each term of the Fibonacci sequence by its remainder on division by 7 we get

$$1, 1, 2, 3, 5, 1, 6, 0, 6, 6, 5, 4, 2, 6, 1, 0, 1, 1, \ldots .$$

The sequence of the first sixteen terms recurs indefinitely and every eighth term is 0. That is, every eighth term of the Fibonacci sequence is a multiple of 7.

3.1

Modulus		Least positive residue	Least absolute residue
7	$1981 = 7 \cdot 283$	0	0
17	$1981 = 17 \cdot 116 + 9$	9	-8
101	$1981 = 101 \cdot 19 + 62$	62	-39

3.2 Putting $k = 12r + 1$, $6k + 5 = 72r + 11$. So

$$6k + 5 = 12(6r) + 11 \equiv 11 \pmod{12}$$

and

$$6k + 5 = 4(18r + 2) + 3 \equiv 3 \pmod 4.$$

3.3 (a) $1^2 \equiv 2^2 \pmod 3$ but $1 \not\equiv 2 \pmod 3$.

(b) $1^2 \equiv 2^2 \pmod 3$ and $2 \equiv 5 \pmod 3$, but $1^5 \not\equiv 2^5 \pmod 3$.

3.4 (a) The last digit of a positive number is its least positive residue modulo 10. So we require the least positive residue of n^4 as n ranges over a complete set of residues of 10, say $n = -4, -3, -2, -1, 0, 1, 2, 3, 4$ and 5. As $r^4 = (-r)^4$ we can overlook the four negative values of n.

$$0^4 \equiv 0 \pmod{10}, \quad 1^4 \equiv 1 \pmod{10}, \quad 2^4 \equiv 6 \pmod{10},$$
$$3^4 \equiv 1 \pmod{10}, \quad 4^4 \equiv 6 \pmod{10} \quad \text{and } 5^4 \equiv 5 \pmod{10}.$$

So the possible last digits of fourth powers are 0, 1, 5 or 6.

(b) If x is a fourth power then $x \equiv 0, 1, 5$ or $6 \pmod{10}$, and so $x \equiv 0$ or $1 \pmod 5$. Hence if n is the sum of three fourth powers then

$$n \equiv \{0 \text{ or } 1\} + \{0 \text{ or } 1\} + \{0 \text{ or } 1\} \equiv 0, 1, 2 \text{ or } 3 \pmod 5.$$

We conclude that a sum of three fourth powers cannot be congruent to 4 modulo 5.

3.5 Establishing that $89 | 2^{44} - 1$ amounts to showing that $2^{44} \equiv 1 \pmod{89}$. Now $2^{44} = (2^{11})^4$, so we first work out the least positive residue of $2^{11} \pmod{89}$:

$$2^{11} = 2048 = 23 \cdot 89 + 1$$

so $2^{11} \equiv 1 \pmod{89}$ and $2^{44} \equiv 1^4 \equiv 1 \pmod{89}$.

To show $2^{48} \equiv 1 \pmod{97}$ we use $2^{48} = (2^3)^{16}$. We start with $2^3 = 8$ and keep squaring modulo 87:

$$\begin{aligned} 2^6 &= 8^2 = 64 \equiv -33 \pmod{97}, \\ 2^{12} &\equiv (-33)^2 = 1089 \equiv 22 \pmod{97}, \\ 2^{24} &\equiv (22)^2 = 484 \equiv -1 \pmod{97}, \\ 2^{48} &\equiv (-1)^2 \equiv 1 \pmod{97}. \end{aligned}$$

3.6 (a) Using the 9-test:

$$1578 \equiv 3 \pmod 9 \text{ and } 34971 \equiv 6 \pmod 9,$$

so $1578 \cdot 34971 \equiv 3 \cdot 6 \equiv 0 \pmod 9$.

Now $5518X238 \equiv 32 + X \equiv 5 + X \pmod 9$, and from $5 + X \equiv 0 \pmod 9$ the only possibility for the digit X is 4.

(b) Using the 11-test:

$$89873569 \equiv 9 - 6 + 5 - 3 + 7 - 8 + 9 - 8 \equiv 5 \pmod{11}$$

and

$$16641 \equiv 1 - 4 + 6 - 6 + 1 \equiv -2 \equiv 9 \pmod{11}.$$

Therefore $89873569 \cdot 16641 \equiv 5 \cdot 9 \equiv 1 \pmod{11}$, and the remainder on dividing the product by 11 is 1.

3.7 Calling the cubic $P(x)$ we show that the congruence $P(x) \equiv 0 \pmod 4$ has no solutions, from which it follows that $P(x) = 0$ has no integer solutions. (The congruences $P(x) \equiv 0 \pmod 2$ and $P(x) \equiv 0 \pmod 3$ each have solutions.)

x	0	1	2	3
$P(x) \pmod 4$	2	1	2	3

3.8 Since N and M comprise the same digits, $N \equiv M \pmod 9$ by the 9-test, and so $9|(N - M)$. Taking the sum of the digits of a number preserves its residue class modulo 9, and so $N - M \equiv X \equiv 0 \pmod 9$, and similarly $Y \equiv 0 \pmod 9$, where Y is the sum of the digits of X.

As N and M are 10-digit numbers, $N - M$ has at most ten digits and so $X \leq 90$ (for at worst all ten digits are equal to 9). Of all positive integers not exceeding 90 the largest possible sum of digits is 17, attained by the integer 89. So $Y \leq 17$.

Now as $N > M$ we know that $X > 0$ and $Y > 0$. Therefore $Y \equiv 0 \pmod 9$ and $0 < Y \leq 17$ give the single possibility $Y = 9$.

3.9 (a)

$$\begin{aligned} 8x \equiv 12 \pmod{60} &\iff 2x \equiv 3 \pmod{15} \\ &\iff 2x \equiv 18 \pmod{15} \\ &\iff x \equiv 9 \pmod{15} \end{aligned}$$

(b)

$$\begin{aligned} 21x \equiv 35 \pmod{47} &\iff 3x \equiv 5 \pmod{47} \\ &\iff 16 \cdot 3x \equiv 16 \cdot 5 \pmod{47} \\ &\iff x \equiv 80 \equiv 33 \pmod{47} \end{aligned}$$

(c)

$$\begin{aligned} 6x \equiv 5 \pmod{41} &\iff 42x \equiv 35 \pmod{41} \\ &\iff x \equiv 35 \pmod{41} \end{aligned}$$

(d)

$$\begin{aligned} 5x \equiv 1 \pmod{93} &\iff 95x \equiv 19 \pmod{93} \\ &\iff 2x \equiv 112 \pmod{93} \\ &\iff x \equiv 56 \pmod{93} \end{aligned}$$

3.10 To solve simultaneously $n \equiv 0 \pmod 9$, $n \equiv 15 \pmod{16}$ and $n \equiv 23 \pmod{25}$, we follow the steps of the proof of the Chinese Remainder Theorem, **B** page 87.

$n_1 = 9,\ n_2 = 16,\ n_3 = 25, \qquad n = 9 \cdot 16 \cdot 25 = 3600.$

$N_1 = 400,\ N_2 = 225,\ N_3 = 144.$

$a_1 = 0,\ a_2 = 15,\ a_3 = 23.$

$$\begin{aligned} N_1x_1 \equiv 1 \pmod{n_1} &\Rightarrow 400\,x_1 \equiv 1 \pmod 9 &&\Rightarrow x_1 \equiv 7 \pmod 9 \\ N_2x_2 \equiv 1 \pmod{n_2} &\Rightarrow 225\,x_2 \equiv 1 \pmod{16} &&\Rightarrow x_2 \equiv 1 \pmod{16} \\ N_3x_3 \equiv 1 \pmod{n_3} &\Rightarrow 144\,x_3 \equiv 1 \pmod{25} &&\Rightarrow x_3 \equiv 4 \pmod{25} \end{aligned}$$

So

$$\begin{aligned} \bar{x} &= a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3 \\ &= 0 + 15 \cdot 225 \cdot 1 + 23 \cdot 144 \cdot 4 = 16623. \end{aligned}$$

The solution of the system is $X \equiv 16623 \pmod{3600}$, and the least positive solution is $n = 2223$.

3.11

$$\begin{array}{llrl} n \equiv 0 \pmod 3 & \Rightarrow & n = 6, 9, 12, 15, 18, & \text{(increasing by 3)} \\ & & \downarrow\quad & \\ n \equiv 3 \pmod 5 & \Rightarrow & n = 18, 33, 48, 63, 78, 93, 108, \ldots & \\ & & \downarrow & \text{(increasing by 15)} \\ n \equiv 3 \pmod 7 & \Rightarrow & n = 108, 213, \ldots & \\ & & \downarrow & \text{(increasing by 105)} \\ n \text{ odd} & \Rightarrow & n = 213. & \end{array}$$

3.12 $$\mathbf{A}^m \cdot \mathbf{A}^n = \begin{pmatrix} u_{m-1} & u_m \\ u_m & u_{m+1} \end{pmatrix} \begin{pmatrix} u_{n-1} & u_n \\ u_n & u_{n+1} \end{pmatrix}$$
$$= \begin{pmatrix} u_{m-1}u_{n-1} + u_m u_n & u_{m-1}u_n + u_m u_{n+1} \\ u_m u_{n-1} + u_{m+1}u_n & u_m u_n + u_{m+1}u_{n+1} \end{pmatrix}$$

and $\mathbf{A}^{m+n} = \begin{pmatrix} u_{m+n-1} & u_{m+n} \\ u_{m+n} & u_{m+n+1} \end{pmatrix}$.

Equating entries in row 2 column 1:

$$u_{m+n} = u_m u_{n-1} + u_{m+1}u_n.$$

Putting $m = n - 1$ gives

$$u_{2n-1} = u_{n-1}^2 + u_n^2,$$

and putting $m = n$ gives

$$u_{2n} = u_n(u_{n-1} + u_{n+1}) = (u_{n+1} - u_{n-1})(u_{n+1} + u_{n-1})$$
$$= u_{n+1}^2 - u_{n-1}^2.$$

4.1 $256^2 < 65621 < 257^2$, and so

$257^2 - 65621 = 428,$

$258^2 - 65621 = 943,$

$259^2 - 65621 = 1460,$

$260^2 - 65621 = 1979,$

$261^2 - 65621 = 2500 = 50^2.$

Therefore $65621 = 261^2 - 50^2 = 211 \cdot 311$, and both of these factors are prime.

4.2 $5^{12} \equiv 1 \pmod{13}$, by Fermat's Little Theorem.

$5^{14} = 5^{12} \cdot 5^2 \equiv 1 \cdot 5^2 \equiv 25 \equiv 12 \pmod{13}.$

$1985^{14} \equiv 9^{14} \equiv 9^{12} \cdot 9^2 \equiv 81 \equiv 3 \pmod{13}$, since $9^{12} \equiv 1 \pmod{13}$.

4.3 $155 = 31 \cdot 5$, $7^{30} \equiv 1 \pmod{31}$ and $7^4 \equiv 1 \pmod{5}$ by Fermat's Little Theorem. Therefore

$$7^{154} = (7^{30})^5 \cdot 7^4 \equiv 1^5 \cdot 7^4 \equiv 18^2 \equiv 14 \pmod{31}$$

and

$$7^{154} = (7^4)^{38} \cdot 7^2 \equiv 1^{38} \cdot 2^2 \equiv 4 \pmod{5}.$$

By the Chinese Remainder Theorem, $x \equiv 14 \pmod{31}$ and $x \equiv 4 \pmod{5}$ has a unique solution modulo 155, which is seen to be $x \equiv 14 \pmod{155}$. So $7^{154} \equiv 14 \pmod{155}$, and the remainder on dividing 7^{154} by 155 is 14.

4.4 If $\gcd(a, 1729) = 1$ then $7 \nmid a$, $13 \nmid a$ and $19 \nmid a$, and so $a^6 \equiv 1 \pmod{7}$, $a^{12} \equiv 1 \pmod{13}$ and $a^{18} \equiv 1 \pmod{19}$. Therefore

$$a^{1728} = (a^6)^{288} \equiv 1^{288} \equiv 1 \pmod{7},$$
$$a^{1728} = (a^{12})^{144} \equiv 1^{144} \equiv 1 \pmod{13},$$

and

$$a^{1728} = (a^{18})^{96} \equiv 1^{96} \equiv 1 \pmod{19}.$$

It follows that $a^{1728} \equiv 1 \pmod{7 \cdot 13 \cdot 19}$.

4.5 By Fermat's Theorem $p^{q-1} \equiv 1 \pmod{q}$, and, since $q | q^{p-1}$,

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{q}.$$

Similarly, $p^{q-1} + q^{p-1} \equiv 1 \pmod{p}$, and therefore

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}, \quad \text{since } \gcd(p, q) = 1.$$

4.6 By the Corollary to Fermat's Theorem, $a^p \equiv a \pmod{p}$, and by Wilson's Theorem, $(p-1)! \equiv -1 \pmod{p}$. Therefore

$$a^p + (p-1)!a \equiv a + (-1)a \equiv 0 \pmod{p}$$

and

$$(p-1)!a^p + a \equiv (-1)a + a \equiv 0 \pmod{p}.$$

4.7 $1 + 2 + 3 + \ldots + (p-1) = p \cdot \frac{p-1}{2}$, and so it suffices to show that $(p-1)! \equiv (p-1) \pmod{p}$ and $(p-1)! \equiv (p-1) \pmod{\frac{1}{2}(p-1)}$. The first of these is precisely Wilson's Theorem, and the second is immediate, since $\frac{1}{2}(p-1)$ divides $p-1$. And so $(p-1)! \equiv p-1 \equiv 0 \pmod{\frac{1}{2}(p-1)}$.

4.8 Since $x^7 \equiv x \pmod{7}$ for all integers x,

$$\begin{aligned} x^9 + 2x^8 + 6x + 5 &\equiv x^3 + 2x^2 + 6x + 5 \\ &\equiv x^3 + 2x^2 - x - 2 \\ &\equiv (x^2 - 1)(x + 2) \pmod{7}. \end{aligned}$$

Since 7 is prime, if $(x^2 - 1)(x + 2) \equiv 0 \pmod{7}$, then either $x^2 - 1 \equiv 0 \pmod{7}$ or $x + 2 \equiv 0 \pmod{7}$ (by Euclid's Lemma). $x^2 - 1 \equiv 0 \pmod{7}$ has solutions $x \equiv \pm 1 \pmod{7}$—and by Lagrange's Theorem there can be no others—and $x + 2 \equiv 0 \pmod{7}$ has the unique solution $x \equiv 5 \pmod{7}$.
So $x^9 + 2x^8 + 6x + 5 \equiv 0 \pmod{7}$ has the three solutions $x \equiv 1, 5, 6 \pmod{7}$.

4.9 (i) $2x^3 + 4x^2 - x + 1 = (2x^2 - 2x + 5)(x + 3) - 14$

$q(x) = 2x^2 - 2x + 5, \quad r(x) = -14.$

(ii) $3x^3 + 1 = (3x + 3)(x^2 - x - 3) + 12x + 10$

$q(x) = 3x + 3, \quad r(x) = 12x + 10.$

4.10 (a) Since $x \equiv 0 \pmod{5}$ is not a solution, we may assume that $x \not\equiv 0 \pmod{5}$, so that $x^4 \equiv 1 \pmod{5}$. Substituting this into the polynomial produces

$$x^3 + x^2 + x + 1 \equiv 0 \pmod{5}.$$

Substituting $x \equiv 1$, 2, 3 and 4 into this polynomial we find three solutions, namely $x \equiv 2$, 3 and 4 (mod 5).

Alternatively: we can make use of factorization:

$$\begin{aligned} x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 & \\ &= (x^4 + 1)(x^3 + x^2 + x + 1) \\ &= (x^4 + 1)(x^2 + 1)(x + 1) \equiv 0 \pmod{5}. \end{aligned}$$

For $x \not\equiv 0 \pmod{5}$, $x^4 \equiv 1 \pmod{5}$ and so $x^4 + 1 \equiv 0 \pmod{5}$ has no solutions.

$x^2 + 1 \equiv 0 \pmod{5}$ has solutions $x \equiv 2, 3 \pmod{5}$.

$x + 1 \equiv 0 \pmod{5}$ has unique solution $x \equiv 4 \pmod{5}$.

As before, there are three solutions $x \equiv 2$, 3 and 4 (mod 5).

(b) $x^{12} - 1 = (x^6 - 1)(x^6 + 1) \equiv 0 \pmod{7}$

$x \equiv 0 \pmod{7}$ is not a solution, but for all other x we know from Fermat's Theorem that $x^6 - 1 \equiv 0 \pmod{7}$. So the congruence has six solutions, $x \equiv 1, 2, 3, 4, 5$ and $6 \pmod{7}$.

(c) $x^5 - x^3 = x^3(x^2 - 1) \equiv 0 \pmod{11}$

$x^3 \equiv 0 \pmod{11}$ has unique solution $x \equiv 0 \pmod{11}$, whilst $x^2 - 1 \equiv 0 \pmod{11}$ has the two solutions $x \equiv \pm 1 \pmod{11}$. So solutions are $x \equiv 0, 1, 10 \pmod{11}$.

(d) $x^5 + x^3 = x^3(x^2 + 1) \equiv 0 \pmod{17}$

$x^3 \equiv 0 \pmod{17}$ has the unique solution $x \equiv 0 \pmod{17}$, whilst $x^2 + 1 \equiv 0 \pmod{17}$ is equivalent to $x^2 \equiv 16 \pmod{17}$ which has the two (and no more, by Lagrange's Theorem) solutions $x \equiv \pm 4 \pmod{17}$. So solutions are $x \equiv 0, 4, 13 \pmod{17}$.

5.1

$$\begin{aligned}\tau(17640) &= \tau(2^3)\cdot\tau(3^2)\cdot\tau(5)\cdot\tau(7^2)\\ &= 4\cdot 3\cdot 2\cdot 3 = 72\\ \sigma(17640) &= \sigma(2^3)\cdot\sigma(3^2)\cdot\sigma(5)\cdot\sigma(7^2)\\ &= \frac{2^4-1}{2-1}\cdot\frac{3^3-1}{3-1}\cdot\frac{5^2-1}{5-1}\cdot\frac{7^3-1}{7-1} = 15\cdot 13\cdot 6\cdot 57 = 66690\end{aligned}$$

5.2 There are eleven ways of expressing 60 as a product of factors exceeding 1, and, accordingly, an integer n with any of the following prime factorizations has $\tau(n) = 60$:

$$p_1^{59},\quad p_1^{29}p_2,\quad p_1^{19}p_2^2,\quad p_1^{14}p_2^3,\quad p_1^{14}p_2p_3,\quad p_1^{11}p_2^4,\quad p_1^9p_2^5,\quad p_1^9p_2^2p_3,\quad p_1^5p_2^4p_3,$$
$$p_1^4p_2^3p_3^2,\quad p_1^4p_2^2p_3p_4$$

The smallest such integer is $n = 2^4\cdot 3^2\cdot 5\cdot 7 = 5040$.

5.3 The divisors of n occur in pairs d, n/d, of which one does not exceed $\sqrt{n}$. Hence the total number of divisors of n is at most $2\sqrt{n}$, that is $\tau(n) \leq 2\sqrt{n}$. However, equality cannot occur, for if each of $1, 2, \ldots, \sqrt{n}$ is a divisor of n then $\sqrt{n}$ is paired with itself $\left(\sqrt{n} = \dfrac{n}{\sqrt{n}}\right)$, and $\tau(n) = 2\sqrt{n} - 1$.

If n is composite then, in addition to 1 and n, n has divisors d and n/d, which may be equal, but one of which is at least $\sqrt{n}$. Therefore $\sigma(n) \geq 1 + n + \sqrt{n} > n + \sqrt{n}$.

5.4 Let $g(n) = \dfrac{f(n)}{n}$, and let $\gcd(r, s) = 1$. Then

$$\begin{aligned}g(rs) &= \frac{f(rs)}{rs} = \frac{f(r)f(s)}{rs}, \qquad \text{since } f \text{ is multiplicative}\\ &= \frac{f(r)}{r}\cdot\frac{f(s)}{s} = g(r)g(s),\end{aligned}$$

showing g to be multiplicative.

5.5 If $n > 6$ is an even perfect number then $n = 2^{r-1}(2^r - 1)$ where $2^r - 1$ is prime, and $r \geq 3$. If r is even then $2^r - 1$ is certainly composite so we confine attention to the case r odd. We shall show that if r is odd then $2^{r-1}(2^r - 1) \equiv 1 \pmod{9}$.

The sequence of powers of 2, when evaluated modulo 9, forms the recurring sequence 2, 4, 8, 7, 5, 1, 2, 4, 8, 7, 5, 1,… . Therefore

	$r \equiv 1 \pmod 6$	$r \equiv 3 \pmod 6$	$r \equiv 5 \pmod 6$
$2^{r-1} \pmod 9$	1	4	7
$2^r - 1 \pmod 9$	1	7	4
$2^{r-1}(2^r - 1) \pmod 9$	1	1	1

In all cases, r odd implies $2^{r-1}(2^r - 1) \equiv 1 \pmod 9$.

5.6 (a) $2 \cdot 4 \cdot 6 \cdot \ldots \cdot (2n) = 2^n \cdot n!$

By Theorem 6-9, the exponent of the highest power of $p \neq 2$ dividing $2^n \cdot n!$ is $\sum_{k=1}^{\infty} [n/p^k]$. The exponent of the highest power of 2 dividing $2^n \cdot n!$ is $n + \sum_{k=1}^{\infty} [n/2^k]$.

(b) $1 \cdot 3 \cdot 5 \cdot \ldots \cdot (2n-1) = \dfrac{(2n)!}{2 \cdot 4 \cdot 6 \cdot \ldots \cdot 2n} = \dfrac{(2n)!}{2^n \cdot n!} = N$

The exponent of the highest power of p dividing N is the difference of the exponents of the highest powers of p dividing $(2n)!$ and $2^n \cdot n!$ By Theorem 6-9, this is

$$\sum_{k=1}^{\infty} [2n/p^k] - \sum_{k=1}^{\infty} [n/p^k], \qquad p \neq 2.$$

The integer N, being a product of n odd integers, is not divisible by the prime 2.

5.7 $\phi(520) = \phi(2^3 \cdot 5 \cdot 13) = 2^3 \cdot 5 \cdot 13 \cdot (1 - \frac{1}{2})(1 - \frac{1}{5}) \cdot (1 - \frac{1}{13})$

$= 2^3 \cdot 5 \cdot 13 \cdot \frac{1}{2} \cdot \frac{4}{5} \cdot \frac{12}{13} = 192$

$\phi(546) = \phi(2 \cdot 3 \cdot 7 \cdot 13) = 2 \cdot 3 \cdot 7 \cdot 13 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{6}{7} \cdot \frac{12}{13}$

$= 144$

5.8 For p prime, $\sigma(p) = p + 1$, $\tau(p) = 2$ and $\phi(p) = p - 1$.

(a) $\tau(p) + \phi(p) = 2 + p - 1 = p + 1 = \sigma(p)$

(b) $\sigma(p) + \phi(p) = 2p = p\tau(p)$

5.9 Since $\gcd(m, n) = 2$, m and n are both even but at least one of them is not divisible by 4. Let us assume, without loss of generality, that $2^2 \nmid n$. Then $m = 2^r m'$ and $n = 2n'$ where m' and n' are odd with $\gcd(m', n') = 1$, and $r \geq 1$. Now

$$\phi(mn) = \phi(2^{r+1} m'n') = \phi(2^{r+1})\phi(m')\phi(n') = 2^r \phi(m')\phi(n'),$$

and

$$\phi(m)\phi(n) = \phi(2^r m')\phi(2n') = \phi(2^r)\phi(m')\phi(2)\phi(n') = 2^{r-1}\phi(m')\phi(n').$$

Therefore $\phi(mn) = 2\phi(m)\phi(n)$.

5.10 If $n-1$ and $n+1$ are both primes ($n > 4$), then n is even and a multiple of 3. So $n = 2^r 3^s M$, where $r \geq 1$, $s \geq 1$, $M \geq 1$ and $\gcd(6, M) = 1$.

Now $\phi(n) = 2^r \cdot 3^S \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \phi(M) = \frac{1}{3} \cdot 2^r \cdot 3^S \cdot \phi(M) \leq \frac{n}{3}$ (since $\phi(M) \leq (M)$.

5.11 $\phi(40) = \phi(2^3 \cdot 5) = 2^3 \cdot 5 \cdot \frac{1}{2} \cdot \frac{4}{5} = 16$. Therefore Euler's Theorem tells us that $13^{16} \equiv 1 \pmod{40}$, and so

$$13^{83} = (13^{16})^5 \cdot 13^3 \equiv 1^5 \cdot 13^3 \equiv 169 \cdot 13 \equiv 9 \cdot 13 \equiv 37 \pmod{40}.$$

The remainder on dividing 13^{83} by 40 is 37.

5.12 $5x \equiv 1 \pmod{28} \quad \Rightarrow \quad 5x \equiv 1 \equiv 29 \equiv 57 \equiv 85 \pmod{28} \Rightarrow \quad x \equiv 17 \pmod{28}$

$25x \equiv 1 \pmod{28} \quad \Rightarrow \quad -3x \equiv 1 \equiv 29 \equiv 57 \pmod{28}$

$\Rightarrow \quad x \equiv -19 \equiv 9 \pmod{28}$

The multiplicative inverses modulo 28 of 5 and 25 are respectively 17 and 9.

$5x \equiv 11 \pmod{28} \quad \Rightarrow \quad x \equiv 17 \cdot 11 \equiv 19 \pmod{28}.$

$25x \equiv 11 \pmod{28} \quad \Rightarrow \quad x \equiv 9 \cdot 11 \equiv 15 \pmod{28}.$

5.13 From the Corollary to Fermat's Theorem, we have $p^q \equiv p \pmod{q}$. But $p^q \equiv p \equiv 0 \pmod{p}$, and so $p^q \equiv p \pmod{pq}$.

Similarly, $q^p \equiv q \pmod{pq}$. Adding the congruences gives

$$p^q + q^p \equiv p + q \pmod{pq}.$$

6.1 By **B** page 184, $2x^2 - 5x + c \equiv 0 \pmod{13}$ has solutions when $(-5)^2 - 4 \cdot 2 \cdot c$ is either a quadratic residue of 13, or is congruent to 0 modulo 13. That is, when

$$25 - 8c \equiv 0, 1, 3, 4, 9, 10 \text{ or } 12 \pmod{13}.$$

As $25 \equiv -1$ and $-8 \equiv 5 \pmod{13}$, that is

$$5c \equiv 1, 2, 4, 5, 10, 11 \text{ or } 0 \pmod{13},$$

giving respectively

$$c \equiv 8, 3, 6, 1, 2, 10 \text{ or } 0 \pmod{13}.$$

Solving for the case $c = 1$,

$$2x^2 - 5x + 1 \equiv 2x^2 + 8x - 12$$

$$\equiv 2(x^2 + 4x - 6) \equiv 2((x+2)^2 - 10) \equiv 0 \pmod{13}.$$

Therefore $(x+2)^2 \equiv 10 \equiv 36 \pmod{13}$, giving

$$x + 2 \equiv \pm 6 \pmod{13}, \quad \text{or } x \equiv 4, 5 \pmod{13}.$$

6.2 (a) $3^{(17-1)/2} = 3^8 = 3^4 \cdot 3^4 = 81 \cdot 81 \equiv (-4) \cdot (-4) \equiv 16 \equiv -1 \pmod{17}$

(b) $3^{(19-1)/2} = 3^9 = 81 \cdot 81 \cdot 3 \equiv 5 \cdot 5 \cdot 3 \equiv 6 \cdot 3 \equiv 18 \equiv -1 \pmod{19}$

3 is a quadratic nonresidue of both 17 and 19.

6.3 Suppose $n > 2$, $\gcd(a, n) = 1$ and $x^2 \equiv a \pmod{n}$. Then $\gcd(x^2, n) = 1$ and so $\gcd(x, n) = 1$. (Any common divisor of x and n also divides x^2.)

Now

$$a^{\phi(n)/2} \equiv (x^2)^{\phi(n)/2} \equiv x^{\phi(n)} \equiv 1 \pmod{n}, \qquad \text{by Euler's Theorem.}$$

A counterexample to the converse is provided by $a = 3$, $n = 8$:

$$a^{\phi(n)/2} = 3^{\phi(8)/2} = 3^{4/2} = 3^2 \equiv 1 \pmod{8}.$$

However, the quadratic residues of 8 are 0, 1 and 4.

6.4 Referring to properties (1) to (6) of the Legendre symbol (**B** pages 192–3),

$(18/19) = (-1/19)$ by (1)

$= (-1)^{(19-1)/2} = -1$ by (5);

$(45/19) = (3^2/19)(5/19)$ by (4)

$= (5/19)$ by (2)

$= (5 \cdot 2^2/19) = (20/19)$ by (6)

$= (1/19) = 1$ by (1) and (5);

$(2/19) = (2 \cdot 3^2/19) = (18/19)$ by (6)

$= -1$ as above.

6.5 Taking the first five squares,

$$(1/29) = (4/29) = (9/29) = (16/29) = (25/29) = 1.$$

Now $(-1/29) = (-1)^{(29-1)/2} = 1$, and so the negative of any quadratic residue of 29 is also a quadratic residue. Taking the negatives of the above five gives three further quadratic residues:

$$(28/29) = (20/29) = (13/29) = 1.$$

Now $28 = 4 \cdot 7$ and $20 = 4 \cdot 5$, so property (6) of the Legendre symbol gives $(7/29) = (5/29) = 1$, and their negatives $(22/29) = (24/29) = 1$. Finally, $24 = 4 \cdot 6$ so we have $(6/29) = 1$ and its negative, $(23/29) = 1$. We have now found 14 quadratic residues of 29, which is known to be the correct total. They are 1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25 and 28.

6.6 By Wilson's Theorem, $(p-1)! \equiv -1 \pmod{p}$.

By Euler's Criterion, $a^{(p-1)/2} \equiv (a/p) \equiv \pm 1 \pmod{p}$, so $(a/p)a^{(p-1)/2} \equiv 1 \pmod{p}$.

Therefore $(p-1)! \equiv -(a/p)a^{(p-1)/2} \pmod{p}$.

6.7 $S = \{7, 14, 21, 28, 35, 42\}$

$\equiv \{\underline{7}, 1, \underline{8}, 2, \underline{9}, 3\} \pmod{13}$

So $(7/13) = (-1)^3 = -1$.

$S = \{11, 22, 33, 44, 55, 66, 77, 88, 99, 110, 121\}$

$\equiv \{11, \underline{22}, 10, \underline{21}, 9, \underline{20}, 8, \underline{19}, 7, \underline{18}, 6\} \pmod{23}$

So $(11/23) = (-1)^5 = -1$.

$S = \{3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42\}$

$\equiv \{3, 6, 9, 12, \underline{15}, \underline{18}, \underline{21}, \underline{24}, \underline{27}, 1, 4, 7, 10, 13\} \pmod{29}$

So $(3/29) = (-1)^5 = -1$.

6.8 We use Theorem 9-6, which tells us that 2 is a quadratic residue of odd prime p if and only if $p \equiv \pm 1 \pmod{8}$.

(a) For $n > 1$, $4^n + 1 \equiv 1 \pmod{8}$.

(b) For $p \geq 3$, $2^p - 1 \equiv -1 \pmod{8}$.

(c) For $n > 1$, $2^{2^n} + 1 \equiv \pmod{8}$.

Since, in each case, 2 is a quadratic residue, -2 will be a quadratic residue precisely when -1 is, and this occurs when $p \equiv 1 \pmod{4}$.

(a) $4^n + 1 \equiv 1 \pmod{4}$, so -2 is a quadratic residue of prime $4^n + 1$.

(b) $2^p - 1 \equiv -1 \pmod{4}$, $p \geq 3$, so -2 is a quadratic nonresidue of prime $2^p - 1$.

(c) $2^{2^n} + 1 \equiv 1 \pmod{4}$, so -2 is a quadratic residue of prime $2^{2^n} + 1$.

6.9 $(35/71) = (7/71)(5/71)$

$= -(71/7)(71/5)$, by GQRL, noting $7 \equiv 71 \equiv 3 \pmod 4$,

$= -(1/7)(1/5) = -1$

$(139/149) = (149/139) = (10/139) = (2/139)\cdot(5/139)$

$= -1\cdot(139/5)$, by Theorem 9-6 and GQRL,

$= -1\cdot(4/5) = -1$

$(1234/4567) = (2/4567)(617/4567) = (617/4567)$, by Theorem 9-6,

$= (4567/617) = (248/617)$ $[7\cdot 617 = 4319]$

$= (4/617)(2/617)(31/617)$

$= (31/617)$, by Theorem 9-6,

$= (617/31) = (28/31) = (4/31)(7/31)$

$= (7/31) = -(31/7) = -(3/7)$

$= (7/3) = (1/3) = 1$

6.10 (a) $2x^2 + x + 1 \equiv 0 \pmod{29}$ has solutions provided $1^2 - 4\cdot 2 = -7$ is a quadratic residue of 29.

$(-7/29) = (22/29) = (11/29)(2/29)$

$= -(11/29) = -(29/11) = -(7/11)$

$= (11/7) = (4/7) = 1 \implies$ solutions exist.

(b) $2x^2 + 3x - 7 \equiv 0 \pmod{101}$ has solutions provided $3^2 - 4\cdot 2\cdot(-7) = 65$ is a quadratic residue of 101.

$(65/101) = (5/101)(13/101) = (101/5)(101/13)$

$= (1/5)(10/13) = (10/13)$

$= (2^2\cdot 10/13) = (40/13) = (1/13) = 1 \implies$ solutions exist.

6.11 (a) If $p = 4k + 3$ then

$$q = 10p + 3 = 40k + 33 = 4(10k + 8) + 1 = 4k' + 1.$$

It follows that p and q cannot both be congruent to 3 modulo 4, and so the quadratic reciprocity law gives

$$(p/q) = (q/p) = ((10p + 3)/p) = (3/p).$$

(b) There are two cases to be considered.

(i) $p = 4k + 1$. In this case $(-1/p) = 1$ and

$$(p/q) = (q/p) = ((10p + 1)/p) = (1/p) = 1.$$

(ii) $p = 4k + 3$. In this case $(-1/p) = -1$, and

$$q = 10p + 1 = 4(10k + 7) + 3 \equiv 3 \pmod 4.$$

So $(p/q) = -(q/p) = -((10p + 1)/p) = -(1/p) = -1$.

So in both cases $(p/q) = (-1/p)$.

6.12 Since $4^n \equiv 4 \pmod{12}$, for all $n \geq 1$, it follows that

(a) $4^n + 1 \equiv 5 \pmod{12}$, for all $n \geq 1$,

(b) $2^p - 1 = 2\cdot 4^{(p-1)/2} - 1 \equiv 2\cdot 4 - 1 \equiv 7 \pmod{12}$, for all $p \geq 3$, and

(c) $2^{2^n} + 1 = 4^{(2^{n-1})} + 1 \equiv 5 \pmod{12}$, for all $n > 1$.

By Theorem 9-10, 3 is a quadratic nonresidue of any prime of one of these forms.

7.1 (a)
$$\left.\begin{aligned} 39 &= 2\cdot 14+11\\ 14 &= 1\cdot 11+3\\ 11 &= 3\cdot 3+2\\ 3 &= 1\cdot 2+1\\ 2 &= 2\cdot 1\end{aligned}\right\} \Longrightarrow \frac{39}{14} = 2+\cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{1+\cfrac{1}{2}}}} = [2; 1, 3, 1, 2]$$

(b)
$$-\frac{41}{37} = -2+\cfrac{1}{1+\cfrac{1}{8+\cfrac{1}{4}}} = [-2; 1, 8, 4] = [-2; 1, 8, 3, 1]$$

(c)
$$\frac{117}{304} = [0; 2, 1, 1, 2, 23] = [0; 2, 1, 1, 2, 22, 1]$$

7.2 (a) $[2; 3, 1, 7]$ has convergents $2, \frac{7}{3}, \frac{9}{4}$ and $\frac{70}{31}$.

(b) $[0; 5, 4, 3, 2, 1]$ has convergents $0, \frac{1}{5}, \frac{4}{21}, \frac{13}{68}, \frac{30}{157}$ and $\frac{43}{225}$.

(c) $[-3; 1, 1, 1, 1, 19]$ has convergents $-3, -2, \dfrac{-5}{2}, \dfrac{-7}{3}, \dfrac{-12}{5}$ and $\dfrac{-235}{98}$.

7.3
$$3.1416 = \frac{31416}{10000}$$
$$\left.\begin{aligned} 31416 &= 3\cdot 10000+1416\\ 10000 &= 7\cdot 1416+88\\ 1416 &= 16\cdot 88+8\\ 88 &= 11\cdot 8\end{aligned}\right\} \Longrightarrow 3.1416 = [3; 7, 16, 11]$$

$$\left.\begin{aligned} 2718 &= 2\cdot 1000+718\\ 1000 &= 1\cdot 718+282\\ 718 &= 2\cdot 282+154\\ 282 &= 1\cdot 154+128\\ 154 &= 1\cdot 128+26\\ 128 &= 4\cdot 26+24\\ 26 &= 1\cdot 24+2\\ 24 &= 12\cdot 2\end{aligned}\right\} \Longrightarrow 2.718 = [2; 1, 2, 1, 1, 4, 1, 12]$$

7.4 (a) $\frac{24}{13} = [1; 1, 5, 2]$ and has convergents $1, 2, \frac{11}{6}$ and $\frac{24}{13}$, so $11\cdot 13 - 6.24 = -1$. This gives $x = -11$, $y = 6$ as one solution of $13x + 24y = 1$ and the general solution is

$$\{x = -11 + 24t,\ y = 6 - 13t\colon t \in \mathbb{Z}\}.$$

(b) $\frac{97}{86} = [1; 7, 1, 4, 2]$ and has convergents $1, \frac{8}{7}, \frac{9}{8}, \frac{44}{39}$ and $\frac{97}{86}$, so $44\cdot 86 - 39\cdot 97 = 1$. This gives $x = 8\cdot 44 = 352$, $y = 8\cdot(-39) = -312$ as one solution of $86x + 97y = 8$. The general solution is

$$\{x = 352 + 97t,\ y = -312 - 86t\colon t \in \mathbb{Z}\}.$$

(c) $\frac{43}{15} = [2; 1, 6, 2]$ and has convergents $2, 3, \frac{20}{7}$ and $\frac{43}{15}$, so $20\cdot 15 - 7\cdot 43 = -1$. This gives $x = -140$, $y = -49$ as one solution of $15x - 43y = 7$, and the general solution is

$$\{x = -140 + 43t,\ y = -49 + 15t\colon t \in \mathbb{Z}\}.$$

7.5 The convergents of $[2; 4, 4, 4, 4, 4, 4, 4]$ are:

$$C_0 = 2,\quad C_1 = \tfrac{9}{4},\quad C_2 = \tfrac{38}{17},\quad C_3 = \tfrac{161}{72},\quad C_4 = \tfrac{682}{305},\quad C_5 = \tfrac{2889}{1292},$$

$$C_6 = \tfrac{12238}{5473},\quad C_7 = \tfrac{51841}{23184}.$$

According to Theorem 13-8, $C_0 < C_2 < C_4 < C_6 < C_7 < C_5 < C_3 < C_1$. These inequalities can be confirmed by evaluating the convergents to eight decimal places. Alternatively, we can verify $a/b < c/d$ by showing $ad - bc < 0$. For instance:

$$12238 \cdot 23184 - 5473 \cdot 51841 = -1$$

(as we know it should, by Theorem 13-7) and

$$51841 \cdot 1292 - 23184 \cdot 2889 = -4,$$

confirm $C_6 < C_7 < C_5$.

7.6 Let $x = [\overline{5; 3, 1}] = [5; 3, 1, x]$. The latter has convergents $5, \frac{16}{3}, \frac{21}{4}, \dfrac{21x + 16}{4x + 3}$, and so $x = \dfrac{21x + 16}{4x + 3}$, giving $2x^2 - 9x - 8 = 0$. The positive root of this quadratic is $x = \dfrac{9 + \sqrt{145}}{4}$.

Now $[\overline{5; 3, 1}] = 5 + \dfrac{1}{[\overline{3; 1, 5}]}$, so $[\overline{3; 1, 5}] = \dfrac{1}{\dfrac{9 + \sqrt{145}}{4} - 5} = \dfrac{\sqrt{145} + 11}{6}$.

$$[0; 1, \overline{5, 3, 1}] = 0 + \cfrac{1}{1 + \cfrac{1}{[\overline{5; 3, 1}]}} = \cfrac{1}{1 + \cfrac{4}{9 + \sqrt{145}}} = \frac{9 + \sqrt{145}}{13 + \sqrt{145}} = \frac{\sqrt{145} - 7}{6}.$$

The convergents of $[-3; 1, 1, \overline{3, 1, 5}]$ are $-3, -2, \dfrac{-5}{2}, \dfrac{-5y - 2}{2y + 1}$, where $y = \dfrac{\sqrt{145} + 11}{6}$, and so

$$[-3; 1, 1, \overline{3, 1, 5}] = \frac{-5\left(\dfrac{\sqrt{145} + 11}{6}\right) - 2}{2\left(\dfrac{\sqrt{145} + 11}{6}\right) + 1} = \frac{-5\sqrt{145} - 67}{2\sqrt{145} + 28}$$

which simplifies to $-\dfrac{71 + \sqrt{145}}{34}$.

7.7 (a) $\sqrt{18} = 4.24\ldots = 4 + (\sqrt{18} - 4)$ $\qquad a_0 = 4$

$$x_1 = \frac{1}{\sqrt{18} - 4} = \frac{1}{\sqrt{18} - 4} \cdot \frac{\sqrt{18} + 4}{\sqrt{18} + 4} = \frac{\sqrt{18} + 4}{2} = 4 + \frac{\sqrt{18} - 4}{2}$$

$a_1 = 4$

$$x_2 = \frac{2}{\sqrt{18} - 4} = \sqrt{18} + 4 = 8 + (\sqrt{18} - 4)$$

$a_2 = 8$

Now $x_3 = \dfrac{1}{\dfrac{\sqrt{18} - 4}{2}}$ $= x_1$, giving $a_3 = a_1$, and then $a_4 = a_2$, etc. The partial denominators 4, 8 recur indefinitely and so $\sqrt{18} = [4; \overline{4, 8}]$.

(b) $\dfrac{1+\sqrt{13}}{2} = 2 + \dfrac{\sqrt{13}-3}{2}$ (where $\sqrt{13} = 3.60\ldots$) $\quad a_0 = 2$

$$x_1 = \frac{2}{\sqrt{13}-3} = \frac{2}{\sqrt{13}-3}\cdot\frac{\sqrt{13}+3}{\sqrt{13}+3} = \frac{\sqrt{13}+3}{2} = 3 + \frac{\sqrt{13}-3}{2} \qquad a_1 = 3$$

$x_2 = \dfrac{2}{\sqrt{13}-3} = x_1$, and we are immediately in a cycle. Therefore

$$\frac{1+\sqrt{13}}{2} = [2;\overline{3}].$$

(c) $\dfrac{4+\sqrt{21}}{5} = 1 + \dfrac{\sqrt{21}-1}{5}$ (where $\sqrt{21} = 4.58\ldots$) $\quad a_0 = 1$

$$x_1 = \frac{5}{\sqrt{21}-1} = \frac{\sqrt{21}+1}{4} = 1 + \frac{\sqrt{21}-3}{4} \qquad a_1 = 1$$

$$x_2 = \frac{4}{\sqrt{21}-3} = \frac{\sqrt{21}+3}{3} = 2 + \frac{\sqrt{21}-3}{3} \qquad a_2 = 2$$

$$x_3 = \frac{3}{\sqrt{21}-3} = \frac{\sqrt{21}+3}{4} = 1 + \frac{\sqrt{21}-1}{4} \qquad a_3 = 1$$

$$x_4 = \frac{4}{\sqrt{21}-1} = \frac{\sqrt{21}+1}{5} = 1 + \frac{\sqrt{21}-4}{5} \qquad a_4 = 1$$

$$x_5 = \frac{5}{\sqrt{21}-4} = \sqrt{21}+4 = 8 + \sqrt{21}-4 \qquad a_5 = 8$$

$x_6 = \dfrac{1}{\sqrt{21}-4} = \dfrac{\sqrt{21}+4}{5}$ (which is the original number) so $a_6 = a_0$,

$a_7 = a_1$, etc., and we are in a cycle. Therefore $\dfrac{4+\sqrt{21}}{5} = [\overline{1;1,2,1,1,8}]$.

7.8 Putting $k = 2$, $\dfrac{e-1}{e+1} = [0;2,6,10,14,18,\ldots]$. The convergents of $\dfrac{e-1}{e+1}$ are $0, \dfrac{1}{2}, \dfrac{6}{13}, \dfrac{61}{132}, \dfrac{860}{1861}, \ldots$

By the Corollary on **B** page 320, $\left|\dfrac{e-1}{e+1} - \dfrac{61}{132}\right| < \dfrac{1}{132\cdot 1861} < 0.000005$, so $\dfrac{61}{132} = 0.46212\ldots$ is correct to five decimal places.

Putting $k = 1$, $\dfrac{e^2-1}{e^2+1} = [0;1,3,5,7,9,\ldots]$. The convergents are $0, 1, \dfrac{3}{4}, \dfrac{16}{21}, \dfrac{115}{151}, \dfrac{1051}{1380}, \ldots$, and as $\dfrac{1}{151\cdot 1380} < 0.000005$, $\dfrac{115}{151} = 0.76159\ldots$ is $\dfrac{e^2-1}{e^2+1}$ correct to five decimal places.

7.9 $\alpha = [1;\overline{3,4,1}] = [1;3,4,1,\alpha]$. The convergents are $1, \dfrac{4}{3}, \dfrac{17}{13}, \dfrac{21}{16}$ and $\dfrac{21\alpha+17}{16\alpha+13}$, and so $\alpha = \dfrac{21\alpha+17}{16\alpha+13}$ or $16\alpha^2 - 8\alpha - 17 = 0$.

$\beta = [1;\overline{4,3,1}] = [1;4,3,1,\beta]$. The convergents are $1, \dfrac{5}{4}, \dfrac{16}{13}, \dfrac{21}{17}$ and $\dfrac{21\beta+16}{17\beta+13}$, and so $\beta = \dfrac{21\beta+16}{17\beta+13}$ or $17\beta^2 - 8\beta - 16 = 0$. Putting $\beta = \dfrac{-1}{\gamma}$ gives $16\gamma^2 - 8\gamma - 17 = 0$, showing that $\gamma = \dfrac{-1}{\beta}$ is the second root of the quadratic satisfied by α. Therefore α and $\dfrac{-1}{\beta}$ are algebraic conjugates.

7.10 To have a purely periodic continued fraction, the irrational number must exceed 1 $\left(\text{which eliminates } \dfrac{-10-4\sqrt{5}}{3}\right)$ and must have algebraic conjugate in the range from -1 to 0 (which eliminates $3+3\sqrt{2}$).

$$\frac{3+\sqrt{15}}{6} = [\overline{1;6}].$$

7.11
$$0 < \left|\frac{a}{b} - \frac{p_n}{q_n}\right| \le \left|x - \frac{a}{b}\right| + \left|x - \frac{p_n}{q_n}\right|$$

$$< 2\left|x - \frac{p_n}{q_n}\right| < 2\left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| \quad \text{(since successive convergents are on opposite sides of } x\text{)}$$

$$< 2\left|\frac{p_{n+1}q_n - p_nq_{n+1}}{q_nq_{n+1}}\right| = \frac{2}{q_nq_{n+1}}.$$

Therefore $0 < \dfrac{|aq_n - bp_n|}{bq_n} < \dfrac{2}{q_nq_{n+1}}$, giving

$$0 < |aq_n - bp_n| < \frac{2b}{q_{n+1}} < 2$$

from which the result follows.

COMMENT To see that the situation depicted in this example can arise, note that 22/7 and 333/106 are successive convergents to π, but 223/71 approximates π more accurately than 22/7. $[22\cdot 71 - 7\cdot 223 = 1.]$

7.12 By Theorem 13-13, a sufficient condition for 17/16 to be a convergent of $\dfrac{2+\sqrt{11}}{5}$ is that $\left|\dfrac{2+\sqrt{11}}{5} - \dfrac{17}{16}\right| < \dfrac{1}{2\cdot 16^2}$. This can be confirmed by use of a calculator, or

$$\left|\frac{2+\sqrt{11}}{5} - \frac{17}{16}\right| = \left|\frac{-53+16\sqrt{11}}{80}\right| = \left|\frac{-53+16\sqrt{11}}{80}\cdot\frac{-53-16\sqrt{11}}{-53-16\sqrt{11}}\right|$$

$$= \frac{7}{80(53+16\sqrt{11})}$$

$$< \frac{7}{80\cdot 98} = \frac{1}{16\cdot 70} < \frac{1}{2\cdot 16^2}.$$

8.1 (a) $\sqrt{24} = [4;\overline{1,8}]$ has convergents $4, 5, \frac{44}{9}, \frac{49}{10}, \frac{436}{89}, \frac{485}{99}, \ldots$.

As $\sqrt{24}$ has period of length 2, the odd convergents $C_1, C_3, C_5, \ldots$ provide solutions of Pell's Equation:

$$5^2 - 24\cdot 1^2 = 1;\quad 49^2 - 24\cdot 10^2 = 1;\quad 485^2 - 24\cdot 99^2 = 1;\quad \ldots .$$

(b) $\sqrt{37} = [6;\overline{12}]$ has convergents $6, \frac{73}{12}, \frac{882}{145}, \frac{10657}{1752}, \frac{128766}{21169}, \frac{1555849}{255780}, \ldots$

As the period of $\sqrt{37}$ has odd length 1, solutions of Pell's equation are provided by $\frac{73}{12}$ and every second convergent thereafter:

$$73^2 - 37\cdot 12^2 = 1;\quad 10657^2 - 37\cdot 1752^2 = 1;$$
$$1555849^2 - 37\cdot 255780^2 = 1;\quad \ldots .$$

8.2 Suppose $x_0^2 - dy_0^2 = -1$. Then

$$(2x_0^2 + 1)^2 - d(2x_0y_0)^2 = 4x_0^2(x_0^2 - dy_0^2 + 1) + 1 = 1.$$

As the period of $\sqrt{74}$ has odd length, $\dfrac{x_0}{y_0} = C_4 = [8;1,1,1,1] = \dfrac{43}{5}$ is a solution of $x^2 - 74y^2 = -1$. Therefore $x = 2\cdot 43^2 + 1 = 3699$, $y = 2\cdot 43\cdot 5 = 430$ is a solution of $x^2 - 74y^2 = 1$.

8.3 $x^2 + 2xy - 2y^2 = (x + y)^2 - 3y^2 = 1$. $\sqrt{3} = [1;\overline{1,2}\,]$ has convergents 1, 2, $\frac{5}{3}$, $\frac{7}{4}$, $\frac{19}{11}$, $\frac{26}{15}$, …, and so the Diophantine equation has solutions

$$x + y = 2,\ y = 1\ (x = 1);\quad x + y = 7,\ y = 4\ (x = 3);\quad x + y = 26,\ y = 15\ (x = 11);\quad \ldots .$$

8.4 From Theorem 11-1, if x, y, z is a primitive Pythagorean triple then $x = 2st$, $y = s^2 - t^2$ where $\gcd(s,t) = 1$ and $s \not\equiv t \pmod 2$. Now $x + y = 2st + s^2 - t^2 = (s + t)^2 - 2t^2$. But $s + t$ is odd, and so $(s + t)^2 \equiv 1 \pmod 8$. If t is even, $2t^2 \equiv 0 \pmod 8$, giving $x + y \equiv 1 \pmod 8$; whilst if t is odd, $2t^2 \equiv 2 \pmod 8$, giving $x + y \equiv -1 \pmod 8$.

Similarly, $y - x = (s - t)^2 - 2t^2$ and the same argument confirms that $y - x \equiv \pm 1 \pmod 8$, whence $x - y \equiv \mp 1 \pmod 8$.

8.5 If a Pythagorean triangle has area equal to its perimeter then there are positive integers x, y and z such that

$$x^2 + y^2 = z^2 \quad\text{and}\quad \tfrac{1}{2}xy = x + y + z.$$

Substituting for z from the second equation into the first:

$$x^2 + y^2 = (\tfrac{1}{2}xy - x - y)^2 = \tfrac{1}{4}x^2y^2 + x^2 + y^2 - xy^2 - yx^2 + 2xy,$$

giving $(x - 4)(y - 4) = 8$.

The two solutions are $x = 12$, $y = 5$, $z = 13$ and $x = 8$, $y = 6$, $z = 10$.

8.6 If $x^8 + y^8 = z^4$, then $(x^2)^4 + (y^2)^4 = z^4$, giving a solution of $x^n + y^n = z^n$ for $n = 4$. By Corollary on **B** page 252, no such integers can exist.

8.7 Suppose that $x_0^3 + py_0^3 = p^2z_0^3$. Then $p|x_0^3$, giving $p|x_0$, and so, putting $x_0 = px_1$,

$$p^3x_1^3 + py_0^3 = p^2z_0^3 \quad\text{or}\quad p^2x_1^3 + y_0^3 = pz_0^3.$$

Now $p|y_0^3$ and so $p|y_0$. Putting $y_0 = py_1$ gives

$$px_1^3 + p^2y_1^3 = z_0^3.$$

But now $p|z_0^3$ and so $p|z_0$. Putting $z_0 = pz_1$ gives

$$x_1^3 + py_1^3 = p^2z_1^3.$$

This is a second solution of the original equation, and so any positive solution must lead to a smaller positive one, in that $0 < z_1 < z_0$. By the method of infinite descent, this is impossible, and so the equation has no positive solutions.

8.8 It is a simple matter to verify that the only solution in positive integers of $u + v = uv$ is given by $u = v = 2$. The corresponding solution of $x^2 + y^2 = x^2y^2$ requires $x^2 = y^2 = 2$, and so there are no solutions in positive integers.
Alternatively: Suppose we have a (positive) solution $x_1^2 + y_1^2 = x_1^2y_1^2$. Then rearranging, $x_1^2 = y_1^2(x_1^2 - 1)$ shows that $y_1^2|x_1^2$. Similarly, from $y_1^2 = x_1^2(y_1^2 - 1)$, we have that $x_1^2|y_1^2$. It follows that $x_1 = y_1$, and the equation becomes $2x_1^2 = x_1^4$ (i.e. $x_1^2 = 2$), which has no solutions. This contradicts the existence of a solution.

8.9 The result is true. If m and n are each sums of two squares then, for any prime p of the form $4k + 3$, the exponent of p is even in the prime factorizations of both m and n. But then the exponent of p in n/m is even, and the result follows from the Corollary to Theorem 12-3.

8.10 We require the three smallest integers greater than 1000 which can be expressed as $4^n(8m + 7)$. Any integer which is congruent to 7 modulo 8 is of this form, and the only other candidates are multiples of 4. Thus:

$1004 = 4 \cdot 251$ and $251 \equiv 3 \pmod{7}$, ×

$1007 \equiv 7 \pmod{8}$. $1007 = 4^0(8 \cdot 125 + 7)$.

$1008 \equiv 4^2 \cdot 63$ and $63 \equiv 7 \pmod{8}$. $1008 = 4^2(8 \cdot 7 + 7)$.

$1012 = 4.253$ and $253 \equiv 5 \pmod{8}$. ×

$1015 \equiv 7 \pmod{8}$. $1015 = 4^0(8 \cdot 126 + 7)$.

The first three are 1007, 1008 and 1015.

Solutions to Section 1.8 (Tape) Problems

Problem 1

Conjecture: $n! > n^3$ for all $n \geq 6$.

Proof (by induction)

$720 = 6! > 6^3 = 216$, so the result is true for $n = 6$.

Suppose $k! > k^3$, for some $k \geq 6$. Then

$$(k+1)! = (k+1)k! > (k+1)k^3.$$

If we can show that $(k+1)k^3 > (k+1)^3$, then the induction step follows and the proof is complete. To show $(k+1)k^3 > (k+1)^3$ we need only show that $k^3 > (k+1)^2$.

$k^3 > (k+1)$

For $k \geq 6$,

$$k^3 = kk^2 > 3k^2 = k^2 + kk + k^2 > k^2 + 2k + 1 = (k+1)^2.$$

Problem 2

(a) By the Division Algorithm, either $n = 2k$ or $n = 2k + 1$.

$$n = 2k \implies n^5 - n = 32k^5 - 2k = 2(16k^5 - k) \implies 2|n^5 - n$$

$$\begin{aligned} n = 2k + 1 \implies n^5 - n &= (2k+1)^5 - (2k+1) \\ &= 32k^5 + 80k^4 + 80k^3 + 40k^2 + 10k + 1 - (2k + 1) \\ &= 2(16k^5 + 40k^4 + 40k^3 + 20k^2 + 4k) \\ &\implies 2|n^5 - n \end{aligned}$$

(b) Conjecture: $30|n^5 - n$, for all integers n.

(Note that $2^5 - 2 = 30$, so no integer exceeding 30 can have this property.)

(c) *Proof* By Corollary 2 (**B** page 28), it suffices to show that $2|n^5 - n$, $3|n^5 - n$ and $5|n^5 - n$, for all integers n. We have already shown $2|n^5 - n$ in part (a).

By the Division Algorithm, n is of one of the forms $3k$, $3k + 1$ or $3k + 2$. In the binomial expansion of $(3k + r)^5$, every term is divisible by 3 except (possibly) the final term r^5. Therefore

$$n = 3k \implies 3|n \implies 3|n(n^4 - 1) \implies 3|n^5 - n$$

$$\begin{aligned} n = 3k + 1 \implies n^5 - n &= (3k+1)^5 - (3k+1) \\ &= 3P_1(k) + 1^5 - 3k - 1 \\ &= 3(P_1(k) - k) \implies 3|n^5 - n \end{aligned}$$

$$\begin{aligned} n = 3k + 2 \implies n^5 - n &= 3P_2(k) + 2^5 - (3k+2) \\ &= 3(P_2(k) - k) + 30 \\ &= 3(P_2(k) - k + 10 \implies 3|n^5 - n \end{aligned}$$

That $5|n^5 - n$ can be proved similarly. However, it follows immediately from the result of SAQ 9 on page 17 of the unit.

If $5|n$ then $5|n(n^4 - 1)$. That is $5|n^5 - n$.

If $5 \nmid n$ then n^4 is of the form $5k + 1$. That is $5|n^4 - 1$, and so $5|n(n^4 - 1)$.

Problem 3

(a) Eliminating x from the pair of equations

$$3x + 7y + 9z = 300 \quad \text{and} \quad 2x + 3y + 5z = 167$$

gives

$$5y + 3z = 99.$$

One solution of this Diophantine equation, $y = 0$, $z = 33$, is easily spotted, leading to the general solution

$$\{y = 3t,\ z = 33 - 5t\colon t \text{ any integer}\}.$$

Substituting back into either of the original equations gives corresponding value $x = 1 + 8t$, and the general solution of the system

$$\{x = 1 + 8t,\ y = 3t,\ z = 33 - 5t\colon t \text{ any integer}\}.$$

(b) For positive solutions we require $t > 0$ and $33 - 5t > 0$. $t = 1, 2, 3, 4, 5$ and 6 are the only values satisfying these conditions, giving six positive solutions of the system.

They are (9, 3, 28), (17, 6, 23), (25, 9, 18), (33, 12, 13), (41, 15, 8) and (49, 18, 3).

Problem 4

(a) Suppose there exist integers x, y and z such that

$$6x + 15y - 18z = 100.$$

3 divides the left-hand side (since it divides each coefficient), but $3 \nmid 100$—a contradiction.

(b) *Conjecture:* If $\gcd(a, b, c) \nmid k$ then the Diophantine equation

$$ax + by + cz = k.$$

has no solution.

Proof Suppose there exist integers x, y and z such that $ax + by + cz = k$, and let $\gcd(a, b, c) = d$. Then $d|a$, $d|b$ and $d|c$, and so $d|ax + by + cz$. That is $d|k$, which is a contradiction.

(c) *Conjecture:* The Diophantine equation $ax + by + cz = k$ has solutions if and only if $\gcd(a, b, c)|k$.

Having seen in (b) that the condition $\gcd(a, b, c)|k$ is necessary for the equation to have integer solutions, we must now show that it is also sufficient. We shall achieve this by proving a generalization of Theorem 2-3 (**B** page 25), namely

Theorem Given non-zero integers a, b and c, there exist integers x, y and z such that

$$\gcd(a, b, c) = ax + by + cz.$$

Proof By Theorem 2-3 there exist integers r and s such that

$$\gcd(a, b) = ar + bs$$

and again by Theorem 2-3 there exist integers u and v such that

$$\begin{aligned} \gcd(\gcd(a, b), c) &= \gcd(a, b)u + cv \\ &= (ar + bs)u + cv \\ &= a(ru) + b(su) + cv. \end{aligned}$$

We claim that $\gcd(a, b, c) = \gcd(\gcd(a, b), c)$, which will complete the proof, for then $x = ru$, $y = su$ and $z = v$ are the required integers. Let $d = \gcd(a, b, c)$ and $d' = \gcd(\gcd(a, b), c)$. Then $d|a$ and $d|b$ implies $d|\gcd(a, b)$. But also $d|c$, and being a common divisor of $\gcd(a, b)$ and c, $d|d'$. On the other hand, $d'|\gcd(a, b)$ implies $d'|a$ and $d'|b$. As, in addition, $d'|c$ we have $d'|d$. Therefore $d = d'$ as claimed. ■

The proof of the conjecture is now easily completed.

If $\gcd(a, b, c)|k$, say $k = n\gcd(a, b, c)$, then by the theorem,

$$n \cdot \gcd(a, b, c) = k = a(nx) + b(ny) + c(nz)$$

gives a solution of the Diophantine equation.

Solutions to Section 3.5 (Tape) Problems

Problem 1

For an integer to be both a square and a cube it must be a sixth power. For any integer a, $a^3 \equiv 0$, 1, or 8 (mod 9) (see SAQ 6). Therefore $a^6 \equiv 0^2$, 1^2 or $8^2 \pmod 9$. That is, $a^6 \equiv 0$ or $1 \pmod 9$.

For any integer a, $a^2 \equiv 0$ or $1 \pmod 4$. Therefore, since $a^6 = (a^2)^3$, $a^6 \equiv 0$ or $1 \pmod 4$.

To be a sixth power, an integer must be congruent to either 0 or 1 modulo 9 and at the same time congruent to either 0 or 1 modulo 4. Working modulo 36, such integers are

$$a^6 \equiv 0, 1, 9 \text{ or } 28 \pmod{36}.$$

Note that $0^6 = 0$, $1^6 = 1$, $2^6 = 64 \equiv 28 \pmod{36}$ and $3^6 = 729 \equiv 9 \pmod{36}$, so all four possibilities do arise.

Problem 2

(i) $$28x \equiv 49 \pmod{53} \iff 4x \equiv 7 \pmod{53}$$
$$\iff 4x \equiv 60 \pmod{53}$$
$$\iff x \equiv 15 \pmod{53}$$

(ii) $34x \equiv 19 \pmod{52}$. Since $\gcd(34, 52) \nmid 19$ this linear congruence has no solutions.

(iii) $$137x \equiv 96 \pmod{19} \iff 4x \equiv 1 \pmod{19}$$
$$\iff 4x \equiv 20 \pmod{19}$$
$$\iff x \equiv 5 \pmod{19}$$

(iv) $$51x \equiv 8 \pmod{53} \iff -51x \equiv -8 \pmod{53}$$
$$\iff 2x \equiv -8 \pmod{53}$$
$$\iff x \equiv -4 \equiv 49 \pmod{53}$$

(v) $$46x \equiv 74 \pmod{98} \iff 23x \equiv 37 \pmod{49}$$
$$\iff 46x \equiv 74 \pmod{49}$$
$$\iff -46x \equiv -25 \pmod{49}$$
$$\iff 3x \equiv 24 \pmod{49}$$
$$\iff x \equiv 8 \pmod{49}$$
$$[\iff x \equiv 8, 57 \pmod{98}]$$

Problem 3

$2x + 3y \equiv 1 \pmod{100}$ (1)

$3x - 2y \equiv 1 \pmod{100}$ (2)

(1) − (2) gives $x \equiv 5y \pmod{100}$.

Substituting in (1) then gives $13y \equiv 1 \pmod{100}$.

$$\begin{aligned} 13y \equiv 1 \pmod{100} \quad &\Longleftrightarrow \quad 91y \equiv 7 \pmod{100} \\ &\Longleftrightarrow \quad -9y \equiv 7 \pmod{100} \\ &\Longleftrightarrow \quad -99y \equiv 77 \pmod{100} \\ &\Longleftrightarrow \quad y \equiv 77 \pmod{100}. \end{aligned}$$

Substituting for y in (2):

$$\begin{aligned} 3x - 154 \equiv 1 \pmod{100} \quad &\Longleftrightarrow \quad 3x \equiv 155 \pmod{100} \\ &\Longleftrightarrow \quad 3x \equiv 255 \pmod{100} \\ &\Longleftrightarrow \quad x \equiv 85 \pmod{100} \end{aligned}$$

Solution $x \equiv 85 \pmod{100}$, $y \equiv 77 \pmod{100}$.

Printed in the United Kingdom by
The Open University